The HP Security Handbook
Protecting Your Business

Governance
Identity Management
Proactive Security Management
Trusted Infrastructure
May 2005

Hewlett Packard

www.hp.com/go/security

HP-PN 5983-0949ENUS

© 2005 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Intel, Xeon, Pentium, and Itanium are trademarks or registered trademarks of Intel Corporation. Microsoft and Windows are registered trademarks of Microsoft Corporation. Other product names appearing in this document may be trademarks or registered trademarks of their corporations.
About HP

HP is a company unlike any other. We serve everyone from consumers to small and mid-sized businesses (SMBs) to enterprises to public sector customers with an extensive portfolio of market-leading solutions specifically designed to meet the needs of each customer segment.

Our annual R&D investment of nearly USD $4 billion fuels the invention of products, solutions, and new technologies. We produce an average of 11 patents a day worldwide. HP Labs provides a central research function for the company which is focused on inventing new technologies to improve our customers' lives, change markets, and create business opportunities.

Millions of people around the world use HP technology every day. HP is:

- the largest consumer IT company
- the world’s largest SMB IT company
- a leading enterprise IT company

Our strategy is to offer high-tech, low-cost products, services and solutions that deliver the best customer experience. Our team of 150,000 employees does business in more than 170 countries. Revenues reached $79.9 billion for the fiscal year that ended October 31, 2004.
HP has a significant presence in all markets we serve

- **Consumer**—leadership in handhelds, notebooks, printers, and digital cameras for rewarding experiences
- **Small and medium business**—market-leading products, solutions, and services for simplified ownership
- **Enterprise**—a full portfolio of leading products and services for building an Adaptive Enterprise
- **Public sector, health, and education**—experience and alliances for lower costs and increased efficiencies

**Doing well by doing good**

HP is proud of our people, our standards and values, and our deep commitment to global citizenship. Since our first year in business in 1939, HP has given back to communities through philanthropic donations of money, equipment, and time.

Today, we employ new models of engagement and new business and technology solutions to help more people around the globe to participate in the world economy via information technology.

Company rankings:

- #1 globally in inkjet, all-in-one, and single-function printers, mono and color laser printers, large format printing, scanners, print servers, and ink and laser supplies*
- #1 globally in x86*, Windows®, Linux®, UNIX®, and blade servers**
- #1 in total disk and storage systems*
- #2 globally in notebook PCs*
- #1 globally in Pocket PCs*
- #1 in customer support**
- #1 position in customer loyalty for ProLiant servers***

For more information, visit [www.hp.com](http://www.hp.com).

**About HP's Security Practice**

HP takes a holistic approach to security that includes the people, process, and technology to ensure the effectiveness of the security solution. HP Services assists to define a security strategy specifically tailored to the customer’s environment and business processes. As a leader in IT management and, specifically, IT service management, HP Services brings tremendous breadth and depth of management expertise to every consulting engagement. Our expert security staff includes Certified Information Systems Security Professionals (CISSPs) and certified Sysadmin, Audit, Network, Security (SANS) individuals who bring extensive experience in multi-vendor platforms including HP-UX, IBM AIX, Sun Solaris, Microsoft Windows, and Linux. As a member of the Information Technology Information Sharing and Analysis Center (IT-ISAC), HP’s security services team stays abreast of the latest information on cyber security issues and utilizes proven best practices and methodologies such as BS 7799/ISO 17799.

---

* Refers to units, except storage referred in factory revenue. Source: IDC Q3 2004
** Source: Gartner, November 2004
*** Source: Technology Business Research, Inc., October 26, 2004
# Table of Contents

**Introduction Letter**                                                                                           .......................................................... i
**Introduction**                                                                                                  .......................................................... ii

**The Changing Security Landscape**                                                                               .......................................................... ii
**HP's Security Framework**                                                                                       .......................................................... iv
  - Business Context                                                                                               .......................................................... iv
  - Governance                                                                                                     .......................................................... v
  - Identity Management                                                                                            .......................................................... v
  - Proactive Security Management                                                                                 .......................................................... v
  - Trusted Infrastructure                                                                                        .......................................................... v

**Security Handbook Contents**                                                                                     .......................................................... v

**Chapter 1 Governance**                                                                                          .......................................................... 1–1

  - **Definition**                                                                                                  .......................................................... 1–2
  - **Purpose**                                                                                                     .......................................................... 1–4
  - **Why Have Governance?**                                                                                       .......................................................... 1–4
  - **The Importance of Information Assets**                                                                          .......................................................... 1–4
  - **Information Security Defined**                                                                                 .......................................................... 1–5
    - Board of Directors Responsibilities                                                                          .......................................................... 1–5
    - IT Responsibilities                                                                                            .......................................................... 1–6
  - **Regulatory Standards**                                                                                       .......................................................... 1–6
    - International Standards                                                                                      .......................................................... 1–7
      - *Control Objectives for Information and Related Technology (COBIT°)*                                       .......................................................... 1–7
      - *Committee of Sponsoring Organizations of the Treadway Commission (COSO)*                                 .......................................................... 1–8
    - When to Use the International Standards                                                                     .......................................................... 1–8
    - *ISO 17799 and BS 7799 Part 2*                                                                                 .......................................................... 1–8
    - *COBIT*                                                                                                       .......................................................... 1–9
    - *COSO*                                                                                                        .......................................................... 1–9
    - Best-Practice Legislation                                                                                     .......................................................... 1–9
    - Privacy Aspects and Issues                                                                                    .......................................................... 1–10
Chapter 2 Identity Management ................................................................................. 2–1

Definition ............................................................................................................. 2–2

Purpose .................................................................................................................. 2–2

What is a Digital Identity? ..................................................................................... 2–4

Managing Identity Data ........................................................................................... 2–4

Multiple Views and Contexts ............................................................................... 2–5

Multiple Levels of Awareness and Control ......................................................... 2–5

Identity Management Components ...................................................................... 2–5

Data Repository Components ............................................................................. 2–6

Security Components ............................................................................................ 2–6

Life Cycle Components ....................................................................................... 2–6

Consumable Value Components ......................................................................... 2–7

Management Components ................................................................................... 2–7

The Effect of Policies on Management Components ........................................... 2–7

Key Elements of Identity Management Solutions ............................................... 2–8

Identity Management Standards .......................................................................... 2–8

Deployment Models .............................................................................................. 2–8

Complexity and Competing Demands .................................................................. 2–9

Numerous Stakeholders ....................................................................................... 2–9

Multiple Domains ................................................................................................. 2–10

Fragmented Implementation .................................................................................. 2–10

Safe Digital Identity Management ....................................................................... 2–10

Product Interoperability Challenges .................................................................... 2–11

Summary of Identity Management Concepts ....................................................... 2–11

HP Identity Management Products and Solutions ............................................... 2–11

Identity Repositories ............................................................................................ 2–11

Types of Directory-Based Identity Repositories ............................................... 2–12

HP and Identity Repositories .............................................................................. 2–12

Security Components ........................................................................................... 2–13

Authentication Technologies .................................................................................. 2–13

Authorization Technologies .................................................................................. 2–16
Chapter 3 Proactive Security Management

Definition

Managing Protection Proactively and Reactively

Responding to Changing Business Models and Threats

Integrating With IT Management

Maintaining Acceptable Security and Risk Levels

Purpose

Protecting Against Increasing Threats

Enabling Changing Trust Models

Combating Increased Process Complexity and Expense

Complying With Changing Regulations

Proactive Security Management Framework

Security Management Processes

Security Management Tools

Gathering and Correlating Security Events

Coordinating and Automating Response to Attacks

Linking to Business Objectives

Enabling Technologies

HP Proactive Security Management Products and Solutions

Security Incident Management Program

Objective

Benefits

Barriers

Defining Information Security Incidents

HP’s Security Incident Management Program

Summary

Security Event Management

Objectives

Environment

Benefits

HP’s Security Event Management Program

HP OpenView for Proactive Security Management

Summary

Security Patch Management

Objectives

Environment

HP’s Patch Management Programs

Summary

Active Countermeasures

History

Technology Overview

Vulnerabilities Addressed
Chapter 4 Trusted Infrastructure ................................................................. 4–1

Definition ................................................................................................................................. 4–2

Purpose ................................................................................................................................. 4–2

Perimeter Security: Keep the Bad Guys Out ................................................................. 4–3

Trusted Infrastructure: Let the Right People In ................................................................. 4–3

Ongoing Evolution ................................................................................................................. 4–4

Infrastructure Technology Directions ................................................................................. 4–4

Network Security Developments ......................................................................................... 4–4

Network Security Architectures ......................................................................................... 4–4

Network-Enforced Security Compliance ............................................................................ 4–4

Host Security Developments ................................................................................................. 4–5

Operating Systems .................................................................................................................. 4–5

Hardware Platforms ............................................................................................................... 4–5

HP’s Strategic Focus .............................................................................................................. 4–6

Achieving Security Through Open Standards .................................................................... 4–6

Trusted Computing for Trusted Infrastructures ................................................................. 4–7

Trusted Computing Products ............................................................................................... 4–7

Trusted Computing Platform Functionality ......................................................................... 4–7

Elements of a More Secure Platform .................................................................................... 4–10

Trusted Computing Across the Infrastructure .................................................................... 4–11

Security and Privacy Issues .................................................................................................. 4–11

Secure Development ............................................................................................................. 4–12

Minimizing Flaws .................................................................................................................. 4–12

Developer Education ............................................................................................................ 4–12

Product Development Life Cycle ......................................................................................... 4–12

Network Security .................................................................................................................. 4–13

Environment .......................................................................................................................... 4–13

Internet Delivery of Services ............................................................................................... 4–13

Telecommuters and Mobile Workers .................................................................................... 4–14

Outsourcing ............................................................................................................................ 4–14

Network Security Analysis and Planning ............................................................................. 4–14

Approach ................................................................................................................................. 4–14

Understanding Security Risks ............................................................................................... 4–14

Understanding and Mitigating Network Security Threats ..................................................... 4–14

Principles of Design ................................................................................................................ 4–17

Securing Network Perimeters and Extranets ...................................................................... 4–18

Virtual Private Networks (VPNs) ......................................................................................... 4–18

Securing Wireless Access ..................................................................................................... 4–19

Device Security ....................................................................................................................... 4–19

Enterprise Requirements ....................................................................................................... 4–20

Best Practices for Secure Networks ....................................................................................... 4–20

Management ........................................................................................................................... 4–20

Operations Security ............................................................................................................... 4–20

Physical Security .................................................................................................................... 4–21

Firewalls .................................................................................................................................. 4–21

Authentication, Authorization, and Auditing (AAA) Servers .................................................. 4–22

Quarantine ............................................................................................................................... 4–22

Summary ................................................................................................................................. 3–21

HP Proactive Security Management Services ...................................................................... 3–21

Proactive Security Management Summary ............................................................................ 3–22
Introduction Letter

In many ways, HP is a unique technology company. No other company develops the same breadth and depth of technology across all market segments—from consumer to enterprise, from small and midsize businesses to the public sector—spanning so many types of computing devices, protocols, standards, and applications. Security is and will remain a prime focus for HP across our complete portfolio.

The HP Security Handbook provides a view of all the different threads of security in which HP works. We plan to update the content regularly; the handbook will be an evolving document that tracks new developments, adds new information as it becomes available, and presents industry standards and initiatives important to security as they mature. Much of the content focuses on the three pillars of HP’s security strategy—identity management, proactive security management, and trusted infrastructures. These are all “big plays”—places where HP believes that we can make a real difference in the way that people use technology.

I cannot think of a bigger challenge than building truly trustworthy infrastructures composed of new hardware architectures, new operating systems, and new applications. Federated identity management will help to liberate users from the tyranny and insecurity of multiple user name and password pairs. And proactive security management is HP’s way of declaring to the security industry that it’s time to stop reacting to threats and begin building intelligence in servers and other network components to better resist unauthorized intrusions. Because HP is such a large company, we have a special responsibility and role within the IT industry to help chart the future, and that’s what the HP security strategy sets out to do. Big plays don’t happen overnight—but these plays form the kernel of our strategy because they are worthwhile and will make a difference.

In addition to describing HP’s security strategy, this handbook illustrates the broad sweep of security activity across the range of the company’s offerings, from services to the fundamental security features incorporated in HP operating systems. It also describes the work of the Trusted Systems Laboratory and how HP researchers look at future challenges. Commentators often say that the only guarantee regarding technology is change; this is especially true for security technology. HP’s investment in research has already provided great benefits, and we expect this trend to continue.

Tony Redmond
Vice President and Chief Technology Officer
HP Services
Introduction

Information security is a fundamental necessity and enabler for modern business. Because information technology infrastructures provide the ability for enterprises to automate, adapt, and accelerate their business strategies, information security is now essential for safeguarding business continuity. Whether enabling secure sharing and collaboration with partners, preventing or detecting insider attacks, or defending against indiscriminant vandalism by unseen and random network attackers—information security is a key element of any IT infrastructure.

Security, however, is not a simple commodity that can be ordered by weight and bolted on to an IT infrastructure. Security considerations should permeate every aspect of IT—from the design of applications and infrastructure to the mechanisms for managing their deployment; from discrete components that protect specific functions to the design of business objectives and the governance of corporate policy; from the management of technology to the management of people.

Measuring security is also difficult—how safe are we at any point? Unlike processor speed or storage capacity, we do not measure security in simple units—except after an incident when we can objectively demonstrate that the deployed security mechanisms are inadequate. As a result, enterprise security has traditionally been mired in a cycle of reactive crises.

The Changing Security Landscape

Enterprises face a rapidly changing environment that demands a proactive stance for information security. Key factors driving this change include:

- Rapid growth in the rate of security incidents throughout the industry
- Ever-increasing sophistication of attack
- Government response through regulation
- Changes in IT infrastructure to accommodate changing business objectives and streamline security processes

Figure i-1
Security Breaches Reported to CERT/CC

![Graph showing security breaches from 1993 to 2003. The total incidents reported in 2003 were 137,529.](attachment:graph.png)
Rapid growth of security incidents. High-profile security breaches have made network security one of the most important concerns for corporate and government networks. Security incidents reported to the CERT® Coordination Center (CERT/CC) rose 2,099 percent from 1998 through 2002—an average annual compounded rate of 116 percent. During 2003 alone, there were 137,529 incidents, up from 82,094 in 2002. Most of these incidents, which can involve from one to hundreds or thousands of sites, resulted from software vulnerabilities. Such vulnerabilities can affect critical infrastructure as well as commerce.

Increasing sophistication of attacks. Although new vulnerabilities have increased only 5 percent in 2003, the vulnerabilities discovered were, and continue to be, more severe, more sophisticated, and much easier to exploit. Recent viruses and worms pose increasingly dangerous threats with new variations of attacks that demonstrate the potential to permanently delete corporate data or shut down entire networks.

Government response through regulation. Governments have not ignored the increasing threat to commerce. Many governmental entities have enacted or are preparing legislation to require business attention to information security issues.

![Sample Regulations Affecting Security](image)

Regulatory mandates such as the Sarbanes-Oxley Act of 2002, the California Database Protection Act of 2001, the Gramm-Leach-Bliley Act (GLB), the Health Insurance Portability and Accountability Act (HIPAA), and the Basel II Accord are an additional catalyst for applying due diligence in the security decision and implementation process. These laws impose strict requirements on enterprises to establish, identify, document, test, and monitor necessary internal control processes. Because information technology supports most, if not all, of these processes, these laws significantly affect companies’ security strategies. These new regulations force security designers and architects to impose and maintain the proper security controls throughout their enterprise.

Changing business objectives and streamlining processes. The need for business agility is driving the development of proactive security capabilities. Ad hoc security implementations often interlock the various components of a business application, which constrains the overall capability to adapt, increases the cost to operate, and often leads to diminishing protection through the lifetime of the application. Enabling rapid flexibility requires an overall process for managing and evolving an organization’s IT security.
HP's Security Framework

Delivering a safer enterprise IT environment requires a framework for rapid and effective response to threats and corporate business objective changes in order to maintain defined levels of security and risk. HP’s security framework, shown in Figure i–3, enables a holistic way to proactively define and deliver security across the enterprise.

The key areas represented in this model include the three areas in which HP is investing to create innovation and differentiation: identity management, proactive security management, and trusted infrastructure. The fourth area, governance, includes the supporting services and tools that HP delivers to ensure that IT security solutions meet business objectives.

Figure i–3
HP’s Security Framework

Business Context

The top level of the security framework consists of business objectives, operational risk, and regulatory and legal compliance. Businesses and organizations have a set of major objectives or missions that drive their existence. In addition, they must manage operational risk and meet regulatory and legal compliance. All of these factors have direct security implications that drive the overall security strategy of a business or organization.

From the security perspective, examples of threats that directly affect the highest levels of a company or an organization include:

- Theft of intellectual property or digital assets
- Disruption of critical services or infrastructure that leads to lost revenues, contractual breaches, or regulatory violations
- Public disclosure of sensitive information, which negatively impacts brand identity or competitive advantage
Governance

Governance refers to the controls and policies that translate high-level business objectives, operational risks, and regulatory needs into the directives, objectives, and policies that drive security mechanisms. Governance is a strategic component of every technology optimization initiative. It includes business logic, business procedures, managerial processes, and operational processes that are all supported by specific, lower-level policies for IT operations and security.

Identity Management

Identity management is the ability to identify every user, application, or device across an organization or business. It provides flexible authentication, access control, and auditing while respecting privacy and regulatory controls. Delivered via a set of processes and tools for creating, maintaining, and terminating a digital identity, identity management allows administrators to manage large populations of users, applications, and systems quickly and easily. The tools permit selective assignment of roles and privileges, which facilitates compliance with regulatory controls and contributes to privacy-sensitive access controls.

Proactive Security Management

Proactive security management focuses on managing security functions in support of business and organizational goals and processes. The fundamental goal of this area is to ensure that protection mechanisms operate appropriately during set-up, operation, and decommissioning of various IT services. Proactive security management:

• Manages the protection of data, applications, systems, and networks, both proactively and reactively
• Supports changing business and organizational models and responds to a changing-threat environment
• Maintains the level of security and operational risk defined by a company or organization

Trusted Infrastructure

Trusted infrastructures are composed of hardware platforms, together with their operating environments and applications, that behave in an expected and predictable way for their intended purpose. Trusted infrastructures must support the IT applications underlying the most critical business processes. When IT infrastructure technologies fail to keep pace with emerging threats, we no longer trust them to sustain the applications we depend on in both business and society.

A trusted infrastructure reliably manages and controls access to information assets while delivering the power required for critical business processes. It helps implement appropriate technologies to secure the end-to-end IT infrastructure of a company or organization, worldwide—including data centers, networks, productivity tools, end-user desktops, and wireless devices.

The need for a trusted IT infrastructure flows from our increasing reliance on IT systems to do everything from running our business to running our society’s utilities. Just as our dependence on IT permeates all aspects of society, security capabilities must permeate all aspects of IT infrastructure. Security must be built-in, not bolted-on, at the platform level, at the network level, and in the very processes used for developing systems.

Security Handbook Contents

HP recognizes the complexity of large, distributed IT environments and takes a proactive approach to enterprise security. Our journey to a secure Adaptive Enterprise is undertaken with planning and preparation, rather than driven by changes in the landscape. This handbook outlines HP’s strategy for information security and summarizes the products, solutions, and services that address the security needs of enterprise customers. It focuses on the three pillars of HP’s security strategy: identity management,
proactive security management, and trusted infrastructures. Along with overarching governance considerations, these three areas bring organizations and companies a safer IT environment that can respond to changing threats and business objectives.

This handbook is intended for CIO’s, security administrators, and other staff who are responsible for their organization’s IT security and infrastructure. Each chapter begins with the definition and purpose of the topic before moving on to discuss details such as the threat environment, related trends, underlying technologies, and challenges. Each chapter concludes with information about solutions that address the security needs discussed.
Chapter 1 Governance

"Director's responsibilities to shareholders and corporate governance legislative guidelines cannot be met unless internal control is based upon rigorous risk assessment, security, and security management and is established by assessing the business impact of loss."

—Joachim Frank, Vice President Enterprise Infrastructure Practice, HP Services Consulting & Integration
The role of governance has never been more critical. Corporate leaders are required to move from a best-practices approach to a legislated approach, and IT departments today are charged with delivering business value with an eye on managing risk as well as establishing, assessing, and reporting against effective business controls. Within HP’s security framework, governance provides the overall structure for implementing business objectives, complying with regulations, adhering to risk strategies, and protecting information assets. Security governance supplies a critical link between business management and IT.

This chapter begins by defining governance and the responsibilities of company officers in meeting legislative requirements. It details the recommended governance life cycle and the steps that need to occur to achieve the objectives of compliance with governance requirements. The chapter ends with a discussion of HP’s Professional Services that encompass the governance life cycle and HP’s vision of the Adaptive Enterprise.

Definition

Governance refers to the controls and policies that translate high-level business objectives, operational risks, and regulatory needs into the directives, objectives, and policies that drive security mechanisms. Governance is a strategic component of every business technology optimization initiative. It contains business logic, business procedures, and managerial and operational processes, which are supported by more specific, lower-level policies for IT operations and security. Governance is often classified as corporate governance, security governance, and IT governance.

Corporate governance is the process by which a company’s board of directors achieves two objectives for shareholders:

- The efficient use of assets for current business
- The availability of assets for new business to maximize shareholder return

Corporate governance achieves these goals by defining the risk profiles of the company’s businesses and investing in the systems, processes, staff, and training needed to operate them. It explicitly defines the risk appetite of the enterprise and the mitigation methods for anticipated and unforeseen risks. These mitigation methods are developed by functional staff (including IT); but the board of directors should review, understand, and agree to them.
Various regulations formalize corporate governance, either specifying adherence to the recognized industry best practices or dictating a very prescriptive process, such as Sarbanes-Oxley. However, complying with regulations does not guarantee good governance. Noncompliance with regulations, on the other hand, is a fairly sure sign of poor governance.

The intent of most regulatory acts such as Sarbanes-Oxley is to remove subjectivity from governance. In the past, codes of practice and best practices have been common methods for demonstrating suitable governance and auditing has been used to prove control. This has been acceptable as long as the results were satisfactory and fraud was not proven. Today, however, regulatory compliance is often perceived as the most important issue. This masks the fact that regulatory compliance is designed to be an indicator of good governance—not good governance in and of itself.

**Security governance** is a component of corporate governance. It is the requirement of company directors to demonstrate due diligence in handling information assets on behalf of stakeholders. Security governance is composed of all the processes and decisions that affect company assets in terms of their validity, confidentiality, integrity, and availability for business. Without security governance, corporate governance objectives cannot be met simply because there can be little faith in the internal control systems.

In this context, security governance encompasses all assets and their threats. Therefore, physical building security and transport security, for example, are part of this process. When assessing risk, the threats to all assets should be reviewed. Some mitigation plans, consequently, will include IT components and some will not. In this sense, security governance is wider in scope than IT governance, as shown in Figure 1–2.

As with corporate governance, mitigation plans for security governance fall within the bounds of the risk appetite as expressed by the board of directors in the company objectives. Likewise, the board should explicitly approve the final choice of mitigation plans and the controls for each.

**IT governance** ensures that IT supports business requirements and that it does so efficiently and flexibly. This subject exists simply because IT and business often misunderstand each other. In particular, the differing time scales, language, priorities, expectations, and contexts of IT and business can lead to a disconnect. The IT Governance Institute (www.itgi.org) is a good source of information about best practices for IT governance and its alignment with security governance. IT governance is directly affected by security governance; IT cannot produce reliable results if security is inadequate.
IT systems, technologies, and processes are at the core of most businesses. As such, they have two important roles: to facilitate business efficiency and to mitigate business risks by implementing controls. Because they have differing impacts, it is important to understand these IT roles.

**Purpose**

Shareholders and legislators can require directors to prove that they have taken due care in the use of company assets. A *company asset* is anything that the company owns and uses in business—from office chairs to information. A lack of security (IT or physical) is usually caused by a lack of due care. To make it easier for company directors to prove due care, every country has a number of legislative frameworks for directors to adhere to—some are statements of self-regulated best practices and others are very prescriptive. If due care cannot be demonstrated, directors can be removed from office, fined, imprisoned, and subjected to the loss of personal property. This occurs in every country in the world today, and it came about long before the Enron scandal broke.

**Why Have Governance?**

Governance regulations and guidelines attempt to provide a prescriptive management framework and an independent method of determining how well businesses are managed. In addition, there is an increasing need for companies to be comparable worldwide. The various stakeholders in a company have differing needs related to governance:

- Shareholders and regulators look for adherence to corporate governance control frameworks and regulations to determine how well the company is managed
- Auditors and regulators refer to demonstrated adherence to security guidelines and control systems to determine whether the company applies basic due diligence and control
- Management follows a security management life cycle to ensure that business controls and IT governance needs are met

**The Importance of Information Assets**

One of the most sensitive areas of modern business is the exposure faced by information assets. In some cases, these assets make up the majority a company’s capital, and their loss or damage can put a company out of business. A graphic example is a credit card company that exposes all of its credit card details such that massive fraud can occur. Such an event exposes the company to legal liability, lost clients, and damages. It would undoubtedly shut the company down and lead to the sanctioning of the company directors for dereliction of duty.

Security governance is comprised of all the actions that directors need to undertake to avoid such events and to prove to authorities, business partners, staff, shareholders, and clients that they are treating company assets in a secure manner. From another viewpoint, if information assets are insecure, IT cannot produce reliable results. Therefore, company directors cannot report accurately or manage assets correctly. Reporting accurately is a key component of Sarbanes-Oxley, the Basel II Accord, and most corporate control frameworks.

In this context, the scope of security governance is the security of operations relating to end products. It is not the security inherent to the product in and of itself. In a financial services business, for example, a credit instrument has the risk that the client will default. This risk falls under corporate governance. However, losing the credit instrument’s details and falsifying transactions are risks within the scope of security governance.
Information Security Defined

Information security refers to the security of information assets. The most widely used characteristics of information security are confidentiality, integrity, and availability:

- **Confidentiality** means that only the user or the user’s delegates have access to the information.
- **Integrity** means that the information is in the expected state and that it has not been changed without knowledge or permission.
- **Availability** means having the information when it is needed.

In reality, availability has the greatest impact. If information is not available and business must continue, is outdated information used instead?

Other characteristics that are commonly referenced include utility (whether information is in a useful state) and non-repudiation (someone who uses the information cannot deny it later). These characteristics are best viewed as consequences or applications of the three basic characteristics. For example, non-repudiation requires an application to use information that can remain confidential, unchanged (integrity), and available in a useful state.

When securing the confidentiality, integrity, and availability of information assets, organizations should examine the entire information environment. This key part of information security is often forgotten. It is common for the IT part of the security equation to be separated financially and organizationally from the wider information security environment, often with dire consequences. For example, information security cannot be guaranteed if:

- Information handling processes are not defined, including backup, restore, and off-site storage procedures for sensitive or critical data
- Audits are not possible because a reliable current state does not exist
- Information-processing facilities do not have adequate physical security and protection, such as appropriate fire suppression systems
- Persons transporting (or with access to) systems or data have not been vetted
- Information life cycle policies and procedures—from creation to destruction—do not exist

These are only examples, and a framework for information security covers most areas. The key is to examine threats to the entire environment and assign mitigation methods and sufficient resources to the totality of the risks. This occurs during the risk assessment process, which should be ongoing.

Board of Directors Responsibilities

Within all aspects of governance, a company’s board of directors is responsible for explicitly defining aspects of control and security. Legislation such as Sarbanes-Oxley requires explicit sign-off. This requirement, however, has existed in the compliance frameworks of most countries for many years, but it was rarely enforced.

Specifically, the governance responsibilities of the board of directors include:

- Understanding the subject of information security in general
- Setting direction and driving policy and strategy
- Defining and agreeing to risk appetite for defined businesses and reviewing and accepting risk mitigation proposals
- Providing resources
• Ensuring that individual roles, responsibilities, and authority are clearly communicated
• Delegating authority, but not responsibility
• Approving security measures explicitly
• Reviewing risk appetite and security measures periodically
• Implementing an organization that enables security governance, with the security department reporting directly to the board and not another business function

The board can delegate these responsibilities, but it is held accountable. For example, outsourcing IT or asset management does not alter the board’s ultimate responsibility for these functions.

IT Responsibilities

By the same token, IT has a number of responsibilities. Its key function is to implement business controls. For this reason, IT should aim to fully understand business objectives. If management and IT are not in alignment (and IT does not fully understand and support the relevant business drivers and priorities), IT will not have the appropriate context in which to frame and plan security architectures.

Specific IT responsibilities for governance include:
• Participating in business impact analysis exercises with business managers
• Proposing and gaining agreement for risk mitigation strategies
• Developing architectures that implement current and potential control requirements
• Identifying threats and analyzing vulnerabilities in proposed technical components, and staying current with updates, patches, and new threat vectors
• Implementing monitoring and incident response methods
• Conducting periodic reviews with audits
• Ensuring application security during development and when acquiring applications externally
• Ensuring awareness of the need to protect information and recommending relevant user training

Due to differing time scales or rapidly changing needs, IT projects may not synchronize with business requirements. Within this context, IT has the responsibility to inform the board of the limits and capabilities of IT and to help improve efficiency in line with business objectives.

Regulatory Standards

Every country has legislation concerning the requirements of directors with regard to due diligence and governance. Although some legislation and standards are very specific, the majority are non-prescriptive guidelines. As a result, most regulatory standards outline directors’ responsibilities without explaining how to accomplish them.

A common theme is an external audit of a control system. The audit is usually of a financial nature to ensure the accuracy of the numbers reported. However, using audit alone as a tool to improve a control system is probably not a good idea. Accounting standards and regulations can be applied worldwide, for example, but they are influenced by local government tax policies. This makes it difficult to compare results.

Another issue with using audit only is the cost associated with control system failures. The cost can be accounted for in many ways, and the manner of accounting can impact an audit. For example, in the past, banks commonly accounted for these failures as operations costs and passed them on. Now banks have a clear obligation to separately report any control system failures that lead to operational losses, in a way that penalizes the bank.
A final difficulty is that audit methods usually audit against a known state. If this state is not defined correctly in the first place, audit is a weak tool for governance. Sarbanes-Oxley is the first framework and legislation that provides enough information for companies to establish a clear control system and track its performance.

Faced with these difficulties, the best course of action is to improve control systems from the bottom up. Conforming to international standards addresses the majority of control system problems. Organizations can then focus on the few remaining concerns.

**International Standards**

Examples that organizations use internationally to demonstrate or regulate governance include: the International Organization for Standardization (ISO) 17799, the Control Objectives for Information and Related Technology (COBIT®), and the Committee of Sponsoring Organizations of the Treadway Commission (COSO).


ISO 17799 is the best practices section of the original BS 7799, which contained two parts: BS 7799 Part 1 (best practices) and BS 7799 Part 2 (security management systems). ISO 17799 recommends best practices for the treatment of information assets using the common characteristics of confidentiality, integrity, and availability.

As an example, the best practices state that a firewall should protect a network perimeter and that a business continuity plan (BCP) should address information availability. However, ISO 17799 does not address how to manage the firewall, when to update the firewall, or what process to use. Similarly, it does not define how to develop or manage a BCP. The reason for this is clear—each company has its own view about the assets to protect and the acceptable risks. It is not easy to define a single management system that can be rigorously applied to all companies. BS 7799 Part 2 does this, but it has not been accepted as an ISO standard.

**Control Objectives for Information and Related Technology (COBIT®)**

COBIT was developed by the Information Systems Audit and Control Foundation (www.isaca.org) and the IT Governance Institute (www.itgi.org). It provides a broad control framework together with control objectives for all of IT. COBIT splits IT into 34 process areas within four domains. There is a four-step cycle from planning through monitoring, and the goal is to provide a control framework that allows management to audit and evaluate how well IT processes align with business.

Only a portion of COBIT focuses on information security, however. It also provides an excellent means of determining the degree of maturity of the control systems within a company. Like ISO 17799, it defines what to do, but not how to do it. COBIT adds the concepts of authenticity and non-repudiation as base requirements within information security, and it uses seven information criteria to define what business requires from IT:

- Effectiveness
- Efficiency
- Availability
- Integrity
- Confidentiality
- Reliability
- Compliance
Committee of Sponsoring Organizations of the Treadway Commission (COSO)

The COSO report defines internal control as a process, affected by an entity’s board of directors, management, and other personnel. It is designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

The COSO framework is mentioned in the Sarbanes-Oxley proposals as a framework suitable to satisfy its requirements, although others such as COBIT also qualify.

The original version of COSO (Internal Control–Integrated Framework) has now been augmented by the addition of the Enterprise Risk Management–Integrated Framework which uses the same conceptual foundations but offers a broad risk-based approach to strategic control. For more details, see [www.theiia.org](http://www.theiia.org).

When to Use the International Standards

ISO 17799 and BS 7799 Part 2

ISO 17799 defines best practices in fairly clear terms and covers ten main areas of business. Following this standard ensures that all areas of a business are reviewed. However, it does not ensure that security is good or sufficient. An assessment against this best-practice framework covers the following ten areas:

- BCP
- System access control
- System development and maintenance
- Physical and environmental security
- Compliance
- Personnel security
- Security organization
- Computer and network security
- Asset classification and control
- Security policy

BS 7799 is often viewed as synonymous with ISO 17799, which is incorrect. BS 7799 Part 2 defines the Information Security Management System and the requirements to make the system work. An external audit can use this framework, but there are important comparability issues. For example, the scope defines which part of a company is reviewed. Unless two companies use an identical scope, there is no comparability. In addition, the Statement of Applicability (SOA) is the management assessment of whether a control is necessary or sufficient. Unless the SOAs are identical, comparability suffers.

Despite these issues, BS 7799 is a useful framework to determine whether security management works. For example, does the organization have a process for policy definition and rollout that works in practice? For more information about BS 7799, visit [www.bsi-global.com](http://www.bsi-global.com).
COBIT

This framework is ideal to review the needs and responsibilities in IT governance from a wider perspective than a pure security view. It takes the position that there are information requirements that align IT with business. The starting point is defining an IT strategic plan. Next, the plan is detailed and the necessary components are acquired and implemented. Finally, the plan is delivered, supported, and monitored.

Handling risk is an implicit understanding within the COBIT framework. However, it does not specifically examine the risk to an information asset and the subsequent mitigation process used by IT. For example, COBIT does not examine the risk of losing an invoicing system at a cost of USD $10,000 per day or the resulting manual and IT mitigation process. Instead, COBIT examines the risk inherent in the IT methods, and using COBIT, a business owner can be sure that an adequate, efficient control system is in place for the IT environment. Note that COBIT is weaker in general security and the process side of IT.

It is often helpful to use the control objectives of COBIT, but to report them within the framework structure of ISO 17799. For more information about COBIT, visit [www.isaca.org](http://www.isaca.org).

COSO

COSO is a comprehensive and fundamental internal control framework. As such, it is an excellent base for corporate governance. For real applicability, however, more specific frameworks and standards need to be used, such as COBIT, ISO 17799 or other best practices that consider the impact of a control. As a general point, it is important to define the impact of a control and determine whether to use it based on the risk it helps mitigate.

Sarbanes-Oxley mentions COSO, but it is not a prerequisite for compliance. Any control system that demonstrates reliable results and follows best practices is suitable. The COSO control framework includes:

- Control environment
- Risk assessment
- Control activities
  - General controls (data center and software access)
  - Application controls (development methodologies and application controls like checksums)
- Information and communication
  - All types, but some focus on control information reports
- Monitoring
  - Continuous
  - Point

COSO is not sufficiently prescriptive to handle security in the broadest sense. There is a strong emphasis on the organizational and cultural requirements to embed risk management and control into a company, but the strong and directive links between risk, risk mitigation, and the mechanisms required in both IT and general security controls have less emphasis. Failure of any part of the underlying security mechanisms that ensure data quality can invalidate the entire control system. A concerted effort is needed to ensure the confidentiality, integrity, and availability of all information assets involved in this equation. For more information about COSO, visit [www.coso.org](http://www.coso.org).

Best-Practice Legislation

The most effective way to ensure that stakeholders such as legislators, auditors, clients, business partners, and staff recognize security governance is to comply with best-practice legislation.
Many legislative texts affect information security, but best-practice legislation requires a complete security governance program for reliable and permanent reporting to regulators. There are a number of important legislative frameworks dealing with different domains and applications, with common threads in terms of controls and best practices:

- Sarbanes-Oxley Act of 2002
- Basel II Accord
- Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Act (GLB)

These texts describe best practices and provide guidelines; however, they do not specify how to comply with them. As an example, the Basel II Accord clearly states the need for business continuity, but it does not provide details or propose the use of a standard body of knowledge, such as the Business Continuity Institute or DRI International.

Faced with this, it is difficult to know how to satisfy regulators. However, as a basis for compliance with best-practice legislation, aiming to comply with the provisions of ISO 17799 and COBIT provides the foundation for compliance with all regulations and for alignment of IT security with business needs.

Privacy Aspects and Issues

Privacy management is a core concern for enterprises and people, and it requires integration with governance efforts. From an enterprise perspective, privacy management is a necessary aspect of regulatory compliance because governments and corporate guidelines require it. Regulatory laws such as Sarbanes-Oxley, GLB, HIPAA, and various governmental directives on data protection require enterprises to implement complex processes to comply with related policies.

Specifically, much work has been done in terms of privacy legislation, often driven by local or geographical needs. This includes European Community data-protection privacy laws, various U.S. privacy laws, and more specific national privacy initiatives. Guidelines are also available for protecting privacy and the flow of personal data, including the Organization for Economic Co-operation and Development (OECD) guidelines. The OECD guidelines describe concepts such as collection limitation, data quality, purpose specification principles, and online privacy policies. For more information about the OECD, visit [www.oecd.org](http://www.oecd.org).

Enterprises store large amounts of personal (confidential) data about their employees, customers, and partners. Failure to comply with privacy policies can result in serious consequences for the reputation and brand of organizations as well as negative legal and financial impacts. Furthermore, a large enterprise with a multi-national presence might need to comply with international privacy laws. Additional nations (such as South America and Japan, where privacy law is coming into effect in 2005) are developing privacy legislation.

Privacy legislation contains common provisions for securely handling, storing, and disseminating information. The same underlying requirements of due diligence for security governance provide the right framework of proof for this aspect of privacy legislation. Because privacy legislation is more closely monitored than governance regulations (any client, employee, or supplier can file a complaint), these security governance practices become mandatory.

The Governance Life Cycle

Ideally, business needs drive the entire governance life cycle. There are many key decisions that only the board of directors or its delegates can make. The board needs to define objectives, identify the risk appetite, and explicitly sign off on mitigation plans for business risks. It must also be aware of the operations of security implementations in terms of how the operations affect governance needs.
It is common for the process of "security" to be technically oriented and not driven from a business perspective. This causes two main problems. First, the security equation focuses on technical assets, rather than all of the assets required to do business. The second problem is that the analysis often examines the cost of mitigation methods (and usually chooses the least expensive) without balancing the cost with the potential business impact. This lack of synchronization often results from the misperception that security is an IT problem or from a communication/organizational gap between business and IT. The need to provide evidence of governance and due diligence via this process is a major requirement.

Another common oversight is driving the process of "security" with security policy. This is a partial mistake. Security policy is derived from an analysis of business needs, and policies are only one of the tools necessary to mitigate risks. Policy should be firmly placed within the mitigation area—if a business asset is of no value, then policies do not need to protect it. Business analysis must be performed to determine how much to spend on risk mitigation, because it corresponds to the business value of the resources being protected.

Figure 1–3 outlines the implementation of security governance in a company, with business needs driving the life cycle.

As shown in this diagram, a company’s board of directors oversees the process. It defines objectives in terms of business, risk appetite, and regulatory requirements. These objectives in turn give a mandate to operational staff to examine the risks and start the life cycle. At least yearly, the board is responsible for explicitly examining audit and test results and determining the appropriate course of action.

The entire life cycle takes place in the background of operations, where mitigation methods are executed. The majority of these methods use IT technologies and processes. IT is responsible for efficiently implementing and managing operations, in line with IT governance principles. IT does not have sole responsibility for
any of the other process steps. However, IT is responsible for providing input and feedback with respect to relevant policies and operations (where appropriate). Continuous open communication and dialogue are keys to ensuring IT alignment with process goals.

In a new company, the ideal first step is to perform a business risk analysis. Subsequent steps might rely on existing architectures and may cause them to be modified. If a business has new risks, for example, it may require new policies or technologies that modify the existing security architecture. The term security architecture as used here implies all of the technology, people, and processes required to implement the security governance objectives of a business and to align these objectives with the requirements of IT governance, due diligence, and legislative compliance.

Existing organizations may choose to start elsewhere in the cycle or with a gap analysis. However, at some stage they must align with the cycle so that the driver is business impact analysis (BIA). It is simply not possible to determine how much money to spend or which mitigation methods are suitable until the potential loss is assessed. The most common mistake, which leads to overspending or underspending, is to drive the life cycle via technology.

Note that the life cycle presented here is a general guide; actions can vary and the content of the steps should be tailored to each organization. Some principles do apply, for example, good governance requires monitoring, a minimum yearly review of risks, and control systems to mitigate those risks.

Gap Analysis

A business that does not have a security architecture or controls is usually characterized by regular spending on a yearly or project cycle basis. From the outside, this looks like a set of remedial actions, rather than a coherent plan. In this case, it is best to start the life cycle by performing a gap analysis, which highlights the differences between the current state and the desired future state.

Many events can trigger the need to do a gap analysis, for example:

- An audit reveals that policy was not followed.
- An intrusion reveals that the network was badly configured.
- A business outage reveals that continuity plan training was not followed properly.

It is not necessary for an event to trigger a gap analysis. A desire to move to a standard can begin a gap analysis against that standard. In addition, a gap analysis can occur at any point during the life cycle—it is not necessarily at the beginning.

Documentation of the current expected state is the critical issue for a gap analysis. Gap analyses often show that the expected state was not documented, or it was well documented some years ago and has evolved since. A simple example is to define and document the current expected working environment of the average PC.

There are many types of gap analyses, including:

- **Standards framework.** In this case, the organization’s desired state is usually a framework such as ISO 17799, BS 7799, COBIT, or COSO. A standards framework measures the state of conformance to the standard. Defining or documenting a current state in order to measure the conformance is not necessary.

- **Policy framework.** Within this framework, an organization’s policies, standards, and guidelines are defined and documented. The policy framework measures their implementation.

- **Audit results.** After an audit, the life cycle process begins by correcting problems or issues identified in the audit results. The audit can be of any kind, including an external audit, a vulnerability test audit, or an intrusion test audit.
Risk Analysis

Risk analysis is the key process step for the governance life cycle. As the normal starting point, risk analysis identifies all business processes and documents the applications and people processes for each. Business management performs the risk analysis to ensure that the perspective is from a business view, rather than from a technical or other view.

Identifying Business Processes and the Impact of Loss

The first step in risk analysis is identifying and prioritizing which business applications and processes are needed to run the business. This makes it easier to define the loss if, for example, a businessperson is asked to quantify an invoicing process or a goods receipt process. It is harder for a businessperson to define the loss of a computer. In addition, doing this from a business view clarifies potential losses and the amount of money required to prevent them.

This step is normally performed through a process of facilitation and questionnaires involving line management of each business function and IT. The result is a list of defined business processes, the losses incurred if the processes are not available, and the timing of the losses. The time factor is important because it affects mitigation. When a business process is lost, the monetary impact does not start immediately. For example, the loss of e-mail has a delayed impact because there are other ways to communicate.

It is helpful to look at all sources of loss to either a business asset or a business process using a loss matrix as illustrated in Table 1–1:

<table>
<thead>
<tr>
<th>Asset or Process</th>
<th>Financial Loss</th>
<th>User Disruption</th>
<th>Legal Impact</th>
<th>Confidentiality</th>
<th>Embarrassment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unavailability</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destruction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For an impact analysis, this matrix can contain financial values or qualitative assessments (for example, high, medium, or low). The use of such a matrix ensures that all of the potential sources of loss are identified. It is easy to forget, for example, that embarrassment due to data modification can cause a real loss to a business.

Identifying Critical Assets

Business management should define the criticality of each business process or application. How long can the business run without the process and, as a direct consequence, without the asset for the process? This ensures that business management drives the requirements and that IT management provides the input for the assets needed.

During this step, the assets used to run each business process are identified. Typically these are IT assets (for example, servers and networks), but they can also be people, processes, and tangible business assets such as buildings and data centers. Certain assets may be required for multiple processes. The intermediate result here is identification of business criticality—either on a subjective scale (high, medium, low, or scored) or an objective scale. Objective figures may be available if a business manager can determine the monetary loss when a process is not available.
Identifying Threats to Assets

For each asset in each business process, the next step is to identify the potential threats to the asset and how often (in probability) they may occur. For ease, it is common to rank the priority of each business asset and deal with the most critical first. A major weakness in this area is that if objective probability data is not available, quantitative methods cannot be used. Qualitative methods should be used instead.

Result

The end result of the risk analysis is a list of business processes, corresponding assets, and the threats to each asset. Table 1–2 gives an example for an invoicing system. The key point here is agreement between business management and IT. Also note that this exercise is qualitative and not quantitative due to a lack of data in most cases.

<table>
<thead>
<tr>
<th>Business Process</th>
<th>Impact of Loss</th>
<th>Impact Starts</th>
<th>Assets</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoicing System</td>
<td>High, $30K per day</td>
<td>After 2 days</td>
<td>Data center</td>
<td>Fire in the computer room</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network infrastructure</td>
<td>Network intrusion</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Windows mail server</td>
<td>System failure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Directory server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Application servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Operations staff</td>
<td>Critical staff missing</td>
</tr>
</tbody>
</table>

Security Control Architecture

This step attempts to determine the residual risk, which is the remaining risk after a mitigation plan is applied, for each threat. There are multiple ways of lowering the impact of a threat, ranging from avoidance to a mitigation plan. Mitigation plans can be based on process or technology. Within the process and technology categories, there are multiple mitigation options with differing effects and levels of residual risk.

Table 1–3 and Table 1–4 outline two examples of threats and the level of residual risk corresponding to the mitigation options for each:

<table>
<thead>
<tr>
<th>Threat</th>
<th>Probability</th>
<th>Business Impact</th>
<th>Mitigation Options</th>
<th>Residual Risk and Cost</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intrusion into the network and loss of data confidentiality</td>
<td>Generally high</td>
<td>Embarrassment, legal action if data is private, governance impact—overall high impact</td>
<td>Firewall at the perimeter</td>
<td>• Low cost but high residual risk&lt;br&gt;• Requires regular updating and the use of good processes</td>
<td>Encryption of all data&lt;br&gt;• High cost, low residual risk&lt;br&gt;• Some application impacts&lt;br&gt;Security policy on data use, labeling of data sources</td>
</tr>
<tr>
<td>Firewalls on all machines</td>
<td></td>
<td></td>
<td></td>
<td>• High cost, medium residual risk</td>
<td></td>
</tr>
<tr>
<td>No access in or out permitted</td>
<td></td>
<td></td>
<td></td>
<td>• Low cost, high business impact</td>
<td></td>
</tr>
<tr>
<td>Network partitioning</td>
<td></td>
<td></td>
<td></td>
<td>• Medium cost, medium residual risk&lt;br&gt;• Requires new management tools</td>
<td></td>
</tr>
</tbody>
</table>
Table 1–4
Threats and Residual Risk After Mitigation, Example #2

<table>
<thead>
<tr>
<th>Threat</th>
<th>Probability</th>
<th>Business Impact</th>
<th>Mitigation Options</th>
<th>Residual Risk and Cost</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invoicing systems unavailable due to denial of service or failure</td>
<td>Medium</td>
<td>Very high</td>
<td>Manual invoicing system</td>
<td>Low residual risk but high cost of implementing and training</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Direct losses sustained due to inability to invoice</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Impacts accounts receivable and direct sales opportunities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hot swap system</td>
<td>Medium cost</td>
<td>Medium residual risk since it covers systems only</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>BCP including all related systems</td>
<td>High cost</td>
<td>Zero residual risk and alignment with governance requirements</td>
<td></td>
<td></td>
<td>BCP plan rehearsals, successful completion of training for all staff</td>
</tr>
</tbody>
</table>

In these examples, there are multiple choices of mitigation and residual risk. The key point of this methodology step is that business managers base their choices on their definition of acceptable residual risk. This is stressed because the choices are often technical decisions.

The output from this step is a set of mitigation choices per threat, an approved set of residual risks, and a set of controls that determine if the mitigation plans are working. In the examples given in Tables 1–3 and 1–4 (see highlights), business management chooses:

- **Example 1.** Encryption of all data: High cost, low residual risk, and some application impacts.
- **Example 2.** BCP including all related systems: High cost but very low residual risk and alignment with governance requirements.

Ideally, for each threat, the business impact, the risk mitigation costs, and the residual risk position should be stated in monetary terms.

**Controls**

When choosing controls, it is common for organizations to have too few and to audit these only. The critical issue is to quantify the impact of a control—either quantitatively (which is difficult due to a lack of data) or qualitatively (which is easier but imprecise). Ideally, each control option has an associated cost and impact. The choice made by business management is based on the cost of the control versus the loss (with no control in place) and the acceptance of the residual risk.

There are many dimensions to controls. Missing just one can mean that the overall control system will not work and security governance will fail. As an example, Figure 1–4 on the following page shows a variety of controls and three examples of their use.

In the case of the physical example, consider the controls necessary to stop someone from entering a building. Normally there is a sign, a door, a lock on the door, an alarm if it is opened, guards behind the door, guards within the building, and if anyone is caught, some kind of sanction. The same set of control types can (and should) be applied to all situations. The remaining examples show how to do this for processes and technical issues.

IT is part of the general concept of business control, because IT exists to implement it. As an example, prior to accounting systems, a business transaction was made in cash or in kind. Control was exercised immediately and the sanction was often severe—especially if a promise was made and not kept. Later, accounting systems were introduced to record transactions. Auditing these transactions on behalf of owners or shareholders followed. However, the basic concept of an invoice to help control the transaction and to ensure payment
remained throughout. The advent of invoicing faster and more efficiently by IT has not changed the underlying purpose, which is to control loss. (No invoicing probably means a loss.) Therefore, the IT-enabled method of invoicing can and should be cost justified in terms of loss.

The same logic applies to e-mail. E-mail helps make business work and implements control. As an example, if an invoice is in error we can use e-mail to communicate. Although it is hard to justify not having e-mail, a different view is necessary when it comes to determining business risks. A business impact analysis of e-mail generally reveals that it is not critical to business because there are other ways to communicate for business purposes. After some time, the lack of e-mail may radically affect a business, but this rarely occurs in the short term. This emphasizes the concept that analyses should always consider the business impact over time.

Security Implementation Architecture

The previous step defines the parameters for a security architecture. The outputs can be technical components, topologies, technical choices, training plans, continuity plans, security policies, process definitions, and job descriptions. All of the outputs must be balanced and implemented to ensure security governance works as planned.

Business management should make all of the choices up to this point. However, the implementation step of the life cycle is a collaboration between operational and IT staff to define the architecture that supports the business choices. The architecture should also produce the controls required for tracking.

At this stage, compromises that require feedback to business management may be necessary, and unforeseen issues may arise that require business decisions. Similarly, some choices will annul others. As an example, a firewall that does not have administration processes defined will soon become useless; the processes and associated costs should be identified. A continuity plan that does not have a process for rehearsing and maintaining it will also become useless. Additional costs identified here can invalidate previous decisions.

This step examines the requirements, defines the overall architecture required, and produces a skeleton or high-level plan. It is important to note that the decisions driving this are business related, not technical, and that the architecture is not fixed in time. It should be designed with an eye to the future. Within this step, it is very important to avoid designing an architecture that is self-defeating in terms of agility and future requirements. For these reasons, defining and following key performance and goal indicators is critical.
Implementation

Operational staff and IT staff drive this step, which takes the output from the previous step and implements it. This is usually a team effort and a multidisciplinary team should drive it. Operations people are principally involved in process design and implementation together with training plan implementation. IT staff implement the approved technical architecture.

As always, additional discoveries may require changes to previous decisions. Under no circumstances should changes be made without business management input. For example, it is common to find residual risk changes at this point. If this occurs, the changes should be presented to business management for a determination of the appropriate course of action. This loop is necessary to align business and IT actions—an essential (and often very difficult) part of governance.

Support, Manage, and Operate

After the overall implementation plan is complete, it is operated as planned. The function here is to execute as agreed. This includes handling events and incidents, managing efficiently, and reporting any issues that could improve efficiency and performance. The objective is not to execute this function as though it were a business with decision-making power of its own. Unfortunately, this improper form of operation frequently occurs.

Audit and Test

This step is actually developed during the previous steps. The ability to test and audit should be identified as one of the control choices. As an example, intrusion detection capability requires technical choices in terms of network topology, components, and machine agents. It is a separate control step because regular action is required. Everything should be tested for intrusion and vulnerability at least once a year, and audit requirements are often shorter. Common sense dictates a quarterly cycle.

Compliance requirements differ based on the industry. In general, Key Performance Indicators (KPIs) will have been chosen and should be monitored or generally available. In a fully agile company, KPIs should be available in close to real time. Given that compliance drives the requirements in many cases, there should be a continuous effort to produce performance reports that support the needs of the approved compliance framework.

Most compliance frameworks are subjective. For practical purposes, there are COSO, COBIT, and ISO 17799/BS 7799. There are also some specific guidelines per industry, but the only one with some degree of prescription is the Basel II Accord, which applies to the finance industry.

Review and Update

The security and governance framework should be formally reviewed and the results documented on a regular basis. A formal review should also occur for a major change in business structure or a new business venture. The documentation demonstrates two objectives: management approval and due diligence to regulators. For this reason, the process should be formal and regular.

The process of review usually includes the risk position and the results of KPIs, audits, and tests. The results should be reviewed at this stage—not delayed until the next review cycle. Actions related to the results of audits, KPIs, and tests should occur as quickly as possible, depending on the nature and severity of the results.
HP Governance Services

Demonstrating security governance is a continuous process. Similar to auditing, most governance frameworks require proof to be presented yearly and in some cases, such as Sarbanes-Oxley, quarterly. HP provides professional services (as well as the necessary hardware and software components when needed) for each step in the governance life cycle. These services include:

Risk Analysis
- Business impact analysis
- Threat analysis
- Training and facilitation
- Physical security and environmental assessment

Security Control Architecture
- Policy development
- Business continuity planning
- Compliance with control frameworks and legislation
- Mitigation planning

Security Implementation Architecture
- Process design and implementation
- Technical design
- Process design including IT Infrastructure Library (ITIL)
- Training

Implementation
- Systems/networks implementation
- Process development
- Training

Support, Manage, and Operate
- IT Service Management (ITSM)
- Incident management

Audit and Test
- Framework gap analysis
- Vulnerability tests
- Intrusion tests
- Compliance tests
- Audit

For further information about HP Professional Services offerings related to governance, see www.hp.com/go/security/governance.
Security and HP’s Vision for the Adaptive Enterprise

To take advantage of new business opportunities as they arise, corporate governance requires efficient asset management and availability. One of the most striking features of today’s business environment is its dynamic nature. Successful companies do capitalize on change, turning what is often unexpected and disruptive into a business advantage. The ability to respond to changes can be summarized into four primary imperatives for business and technology: mitigate risk, maximize financial return, improve performance, and increase agility. As shown in Figure 1–5, these four imperatives are interlocked; they simultaneously apply to all governance decisions.

A company cannot operate without governing security. However, a company that does not govern security so that it is flexible and agile cannot operate efficiently or react in a timely manner to new business opportunities. Companies need to be adaptable and secure to ensure good corporate governance. This is not a choice. The road to corporate governance and compliance with regulations requires that security governance is demonstrable and that adaptability is a reality.

An Adaptive Enterprise is an enterprise that synchronizes business and IT to capitalize on change. Building an Adaptive Enterprise is a transformational journey. This journey excludes the long-term use of ad-hoc, built-to-fit responses to tactical emergencies; decisions must be made in the context of corporate priorities and the transformational roadmap. This roadmap is created after an assessment of the enterprise’s agility today and the most important gaps to address. The roadmap is maintained through the governance life cycle, based on the objectives issued by the board as well as the analysis of the current and future states.

One of the key elements in the transformational journey is to break down implementation silos. Ad-hoc security implementations should be migrated to security services used horizontally across the enterprise and managed in a consistent, secure, and auditable manner. This applies to infrastructure and application control points, for both the service delivery and the service delivery management environments. In particular, the process through which exceptions are managed should be carefully engineered and strictly followed; failure to do so impacts both the ability to adapt and the overall level of protection provided by the control mechanisms in place. This is not just a question of technology; people and processes play a central role in the implementation of the transformational journey.
Governance Summary

Business objectives need to drive security governance. Likewise, mitigation plans and the costs of such plans should be based on business impact or loss potential. This ensures alignment of costs and time horizons with business needs. Mitigation plans for business risks will always be a combination of technology, people, and process. And the majority of these plans are managed and implemented by IT. Because most mitigation methods rely upon IT technologies and processes, joint teams from business operations and IT should determine the mitigation plans to respond to business risks.

Achieving compliance with regulations calls for good control systems, in general. Building good control systems requires organizations to lay the foundation correctly. Aligning with best practices such as COBIT and ISO 17799 facilitates this process.

HP’s Security Governance Services include a broad set of offerings delivered across the governance life cycle to build an enterprise-wide policy foundation, a secure and agile architecture, and an organizational structure. Together these services enable businesses to manage the risks associated with their information assets.
Chapter 2 Identity Management

"Identity management, user provisioning and single sign on are the top three priorities of IT spending in Fortune 1000 companies."


"Digital identity is one of the fundamental building blocks for the next generation of information systems."

— Tony Scott, CTO of General Motors

"The increasingly distributed nature of corporate networks, the proliferation of Web-based applications, increased security awareness, and government regulations such as Sarbanes-Oxley & HIPAA have contributed to making Identity Management a necessity for virtually every business."

— Roberta Witty, Research Director, Gartner, Inc.
Identity management is one of the three key areas in which HP is investing to create innovation and differentiation. Within the HP security framework, identity management is supported by processes and tools that allow administrators to manage large populations of users, applications, and systems quickly and easily. In addition, business policies, regulatory compliance, and risk factors shape the policies and practices that direct identity management.

This chapter begins by providing the definition and purpose of identity management. Next, it presents background information, including identity data management, identity management components, and key elements of identity management solutions. The final section of the chapter discusses the specific identity management capabilities that HP delivers.

**Definition**

Identity management is the set of processes, tools, and social contracts surrounding the creation, maintenance, and use of digital identities for people, systems, and services. It enables secure access to a set of systems and applications. Its components include data repositories, security, life cycle management, consumables, and management policies. Identity management has strong links to security, trust, and privacy management. It also delivers components of risk management.

Traditionally, identity management has been a core component of system security environments. It is used for maintaining account information and controlling access to a system or limited set of applications. Control is usually the primary focus of identity management. For example, an administrator issues accounts to restrict and monitor access to resources. More recently, however, identity management has also become a key enabler of electronic business.

**Purpose**

Identity management combines processes and technologies to secure and manage access to an organization’s resources. In addition, it identifies every user, application, or device throughout and across organizations over time. Identity management provides flexible authentication, access control, and auditing while respecting privacy and regulatory controls. Today, identity management systems are fundamental to establishing accountability in business relationships, customizing the user experience, protecting privacy, and adhering to regulations.
The following list provides examples of the primary goals that drive organizations to implement identity management solutions:

- Reduce total cost of ownership (TCO) for all systems, including the costs of administration, help desk, and technical support
- Reduce management overhead
- Provide competitive advantage by enabling automation and streamlining optimization of business processes
- Improve customer and employee service, and maintain the control and confidentiality of customers, suppliers, and employees
- Reduce the time for new employees to gain access to required organizational resources
- Reduce the risk of using incorrect information for business processes
- Reduce the risk of former employees retaining access to organizational resources
- Support legal and compliance initiatives related to employee and customer data, for example, the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, the EU Directive on Data Protection, the Basel II Accord, and the Canadian Privacy Act

In short, the purpose of identity management is to provide organizations with the following key benefits:

- Enhanced enterprise agility and productivity
- Increased IT management efficiency, including cost reduction
- Effective regulatory compliance
What is a Digital Identity?

Identity is a complicated concept with many nuances that range from the philosophical to the practical. In the context of identity management, however, the identity of an individual is the set of information known about that person. In the digital world, a person's identity is typically referred to as a digital identity. Different contexts, roles, affiliations, and application environments can require different levels of assurance and digital identities. Therefore, a person can have multiple digital identities.

Although digital identities are predominantly associated with humans, they will be increasingly associated with non-human entities (services, systems, and devices) that could act on behalf of people. Specific examples include trusted platforms, next-generation mobile phones, and Digital Rights Management (DRM)-based devices.

Figure 2–2 on the previous page illustrates the content of a digital identity. Identity consists of a person’s unique profile data, identifier data, and authentication and authorization data. Each content piece can be linked to different contexts (company, web, and application) and the person’s role in that context.

Managing Identity Data

Metadata qualify all identity data, and an organization’s policies for identity, authentication, authorization, and privacy protection define the metadata requirements. Policies are defined by an organization’s IT and business decision makers—they are aligned with corporate governance rules, regulatory restrictions, and contractual obligations specific to the organization’s operating environment.

Identity information and related policies can change over time. This means that identity management not only deals with static information but also copes with changes to identity data. The same is true for security policy management.
Multiple Views and Contexts

Identity information can have multiple views. Each view defines a digital identity that is valid and appropriate based on the context or purpose. Using multiple views within and across multiple contexts enables interactions and transactions. Examples of different views and contexts are illustrated in Figure 2–3.

Different stakeholders can disclose, access, and use digital identities in one or more contexts, including personal, social, e-commerce, enterprise, and government. The process occurs through a variety of means including personal appliances, enterprise systems, and web services.

Multiple Levels of Awareness and Control

From the viewpoint of identity subjects, identity information has several levels of awareness and control:

- **Me Me** is the part of identity information that the subject is aware of and directly controls. An example is personal address information stored and maintained in an organization’s white pages directory. It can also include personal or private information—such as a credit card number or Social Security number—that an individual carefully protects and reveals only in particular circumstances.

- **Known Me** is the part of identity information that the subject is aware of and indirectly controls. An example is an individual’s revenue data and associated tax levels that are stored in the tax department’s database. Even though an individual provides the revenue data to the tax department, he or she doesn’t have direct control of the content in the database.

- **Unknown Me** is the part of identity information that the subject is not aware of and cannot control. Other stakeholders, which may be known by the subject, can control this information. Examples include Certification Authorities (CAs), authorized e-commerce sites, Trusted Third Parties (TTPs), and unknown third parties (for example, credit rating agencies and identity thieves).

Identity Management Components

Identity management solutions are modular and composed of multiple service and system components. This section outlines the components of an example identity management solution, as illustrated in Figure 2–4.

![Identity Management Components Diagram](image-url)
Components of identity management solutions exist at different maturity stages. Components like authentication and directories are quite mature and are considered consolidated technologies. Provisioning, authorization, and single sign-on (SSO) are rapidly consolidating. Others, such as privacy and longevity, are still in a definition and research stage.

Data Repository Components

Directory services and meta-directories deal with the representation, storage, and management of identity and profiling information. They provide standard Application Program Interfaces (APIs) and protocols for information access. Data repositories are often implemented as a Lightweight Directory Access Protocol (LDAP)-accessible directory, meta-directory, or virtual directory. Other repositories that are used in the context of identity management solutions are databases and XML-formatted files. Policy information, which governs access to and use of information in the repository, is generally stored in these repositories as well.

Security Components

Authentication providers, sometimes referred to as identity providers, are responsible for performing the primary authentication that links an individual to a given identity. The authentication provider produces an authenticator—a token allowing other components to recognize that primary authentication has been performed.

Primary authentication techniques include mechanisms such as password verification, proximity token verification, smart card verification, biometric scans, and even X.509 public key infrastructure (PKI) certificate verification. Each identity may be associated with multiple authentication providers. In addition, the mechanisms employed by each provider may be of different strengths. To accept the claim of a given identity, some application contexts may require a minimum level of strength.

Authorization providers enforce access control when an entity accesses an IT resource. Authorization providers allow applications to make authorization and other policy decisions based on privilege and policy information stored in the data repository. An authorization provider can support simple access control management at the operating system (OS) level. It can also support sophisticated controls at the application and service levels.

Auditing providers supply the mechanism to track how information in the data repository is created, modified, and used. This is an essential enabler of forensic analysis, which helps determine who circumvented policy controls and how the controls were evaded.

Life Cycle Components

Provisioning is the automation of all the procedures and tools used to manage the life cycle of an identity. Provisioning procedures include:

- Creating the identifier for an identity
- Linking to authentication providers
- Setting and changing attributes and privileges
- Decommissioning an identity

In large systems, provisioning tools generally permit some form of self-service for creating and maintaining an identity. They frequently use a workflow or transactional system to verify data from an appropriate authority. The tools may also propagate data to affiliated systems that may not directly consume the repository.
Identity Management tools create the historical record of an identity. These tools allow the examination of the evolution of an identity over time. Longevity is linked to the concept of attestation—the ability to determine which “actors” had access to which resources and in what timeframe (irrespective of whether they exercised access, which is a matter of auditing).

**Consumable Value Components**

**Single sign-on (SSO)** allows a user to perform a single primary authentication for access to the set of applications and systems in the identity management environment.

**Personalization** and preference management tools associate an identity with application-specific and generic information. These tools allow applications to tailor the user experience, streamline the user interface, and target information dissemination for a business.

**Self-service** enables users to self-register for access to business services and manage profile information without administrator intervention. It also allows users to manage authentication credentials; for example, assigning passwords, resetting passwords, and requesting X.509 PKI certificates. Self-service reduces IT operation costs, improves customer service, and improves information consistency and accuracy.

**Management Components**

**User management** provides IT administrators with a centralized infrastructure for managing user profile and preference information. User management enables organizations to decrease overall IT costs through directory optimization and profile synchronization. These tools provide user self-service capabilities and enhance the value of an organization’s existing IT investments.

**Access management** provides IT administrators with a centralized infrastructure for managing user authentication and authorization. An access control management service increases security, reduces complexity, and reduces overall IT costs by automating access policies for employees, customers, and partners.

**Privacy management** assures that identity management solutions respect privacy and data protection policies as defined in company, industry, and governmental regulations.

**Federation management** establishes trusted relationships between distributed identity providers. This often involves sharing web service endpoints, X.509 PKI certificates, and supported/desired authentication mechanisms.

**The Effect of Policies on Management Components**

Policy controls govern and drive management components. Policies may cause events to be audited or an identity subject to be notified when information is accessed.

- **Identity policies** control the format and lifetime of an identity and its attributes.
- **Authentication policies** control the characteristics and quality requirements of authentication credentials.
- **Authorization policies** determine how resources can be accessed.
- **Privacy policies** govern how identity information may be disclosed.
- **Provisioning policies** determine what resources are allocated to which identities and how the resources are allocated and deallocated.
Key Elements of Identity Management Solutions

Today, there are many products and solutions available in the identity management market. They generally provide one or more of the identity management components and target different types of users and contexts, including e-commerce sites, service providers, enterprises, and government institutions. Key IT industry players are currently focusing on creating identity management suites that provide all of the components shown in Figure 2–4.

There is a considerable amount of overlap between the different solution categories available on the market. A good example is meta-directories and provisioning solutions. The role of meta-directories has gradually shifted from pure data synchronization (a repository function) to life cycle component functions for the creation of user entries (a provisioning function).

Identity management solutions also involve other stakeholders. These include authentication devices (smart cards, biometric devices, and authentication tokens); anonymity services; cryptographic alternatives to RSA-based cryptographic schemes (Identifier Based Encryption [IBE] and trusted platforms); and the standards outlined in the next section.

The quality of identity management products and solutions depends on how successfully they handle a number of factors. Among other things, these factors include keeping identity information in a consistent and up-to-date state, satisfying related management policies and legal requirements, preserving privacy and trust, and ensuring that security requirements are fulfilled.

The key elements to consider in an identity management solution include:

- Adherence to identity management standards
- Types of deployment models
- Means of addressing complexity and competing demands
- Methods of safe digital identity management
- Level of product interoperability

Identity Management Standards

Standards provide a common set of protocols, semantics, and processing rules that allow the various components of an identity management solution to interoperate. Table 2–1 provides an overview of the most important current and emerging standards used in an identity management architecture.

Deployment Models

Identity management systems are primarily deployed in one of three models: silos, walled gardens, or federations.

Silos are the predominant model on the Internet today. In this model, the identity management environment is established and operated by a single entity for a fixed user and resource community. A good example is a Microsoft® Windows® domain governed by a set of predefined administrators and domain controller servers.

Walled gardens represent a closed community of organizations. A single identity management system serves the common user community of a collection of businesses. Most frequently, this occurs in business-to-business exchanges, and specific rules govern the entity operating the identity management system. A good example is the Identrus PKI, which brings together individual bank-level PKIs into a closed banking-community PKI.
<table>
<thead>
<tr>
<th>Type</th>
<th>Relevant Standards</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ISO/ITU x.500</td>
<td><a href="http://www.itu.int">www.itu.int</a></td>
</tr>
<tr>
<td>Authentication Mechanisms</td>
<td>Standardized authentication protocols: Kerberos, SSL/TLS, Public Key Infrastructure (PKI)</td>
<td><a href="http://www.openauthentication.org">www.openauthentication.org</a></td>
</tr>
<tr>
<td></td>
<td>Open Authentication Initiative</td>
<td></td>
</tr>
<tr>
<td>Privacy Standards</td>
<td>Platform for Privacy Preferences (P3P)</td>
<td><a href="http://www.w3.org/P3P">www.w3.org/P3P</a></td>
</tr>
<tr>
<td></td>
<td>Liberty Alliance Standards</td>
<td><a href="http://www.projectliberty.org">www.projectliberty.org</a></td>
</tr>
</tbody>
</table>

**Federations** and federated identity management environments are emerging deployment models. They include systems like the Liberty Alliance Project (endorsed by HP) and systems built on the Web Services Security (WS-Security) standards, the development of which is driven by Microsoft Corporation and IBM Corporation.

The central difference between federated identity management systems and walled gardens is that a single entity operates a walled garden. By contrast, federated systems support multiple identity providers and a distributed and partitioned store for identity information. Clear operating rules govern the various participants in a federation—both the operators of components and the operators of services rely on the information provided by the identity management system. Most systems exhibit strong end-user controls over the dissemination of identity information to members of the federation.

**Complexity and Competing Demands**

The current identity management landscape is very complex because of the multiple interests, perspectives, concerns, and technologies that are involved. Identity management is important in different contexts, including enterprise, e-commerce, and government. It supports business processes and services, and it enables digital interactions and transactions.

There are competing demands on what identity management should provide, differing concerns about its focus, and conflicting interests. Examples of competing demands include enterprise focus versus consumer focus, mobility versus centralization, legislation versus self-regulation, subjects’ control versus organizations’ control, and privacy versus free market.

**Numerous Stakeholders**

Demands are dictated by various stakeholders, which can include enterprises, e-commerce sites, service providers, government agencies, and identity subjects (consumers). Stakeholders have different objectives and priorities when dealing with the management of digital identities:

- **Enterprises** are driven by their business objectives and needs. They manage large sets of identity data to enable their businesses, rationalize their assets, simplify interactions with partners and customers, ensure regulatory compliance, and meet contractual obligations. Identity data also helps enterprises manage the information life cycle of their workforce and manage access to enterprise resources.
• **E-commerce sites and service providers** manage consumers’ identity information to achieve a variety of goals, such as increasing sales, understanding customers’ needs, customizing services, and selling information to third parties.

• **Government agencies** are concerned with the control and protection of their citizens’ personal information. They also seek strong and undeniable authentication mechanisms and the automation and rationalization of their services via the web and the Internet.

• **Consumers** have different concerns and needs depending on the role they play. They are in the middle (or, depending on the point of view, the source) of most of the competing demands previously noted. As employees or consumers, they want to access and use services in the simplest and most efficient way. Private citizens’ needs and concerns might include privacy, distrust of institutions, and the accountability of the involved parties.

This variety of interests and concerns, along with emerging technologies, increases the complexity of identity management. All of these aspects influence each other, via a spiral of potentially conflicting requirements. For example, new legislation addresses citizens’ needs for privacy; however, it constrains how enterprises, service providers, and e-commerce sites process personal information.

**Multiple Domains**

Multiple domains can also increase the complexity of identity management. Business tasks, digital interactions, and digital transactions can span multiple domains. In an e-commerce context, for example, a digital transaction might require the involvement of identity e-commerce sites and the exchange of identity information among these sites. This exchange has strong implications for managing trust, privacy, authentication, authorization, and accountability. Business-to-business interactions and transactions within supply-chain communities face similar challenges as a result of multiple domains.

**Fragmented Implementation**

Further complexity derives from the challenge of installing, configuring, administering, and integrating current identity management products. This is mainly due to the fragmentation of identity management components and the lack of interoperability and standards. This complexity creates frustration and delays the adoption of identity management solutions in the IT environment.

**Safe Digital Identity Management**

Identity management systems bring great value to the digital world. Federated identity environments, in particular, hold promise for widespread deployment. As the distinction between real-world identity and digital identity blurs, however, methods of safe digital identity management need to be considered:

• **Authenticity of identity.** How is the accuracy and validity of identity information measured and determined? What trust services are necessary to generate confidence in information in the identity management system?

• **Longevity of information.** Do identity management systems adequately track changes to identity information over time? Do they maintain the necessary artifacts to support historical investigations?

• **Privacy.** Do identity management systems provide adequate controls to preserve individual privacy? Does the system provide adequate support for anonymity and multiple user-controlled personas?

• **Identity theft.** Do widespread identity management systems make it easier to perpetrate identity theft or identity fraud?

• **Legal structures.** What protections exist for the holder of the identity or the relying party? Do these protections go beyond contractual obligations when digital identity systems are used for interactions that are limited to the physical world today?
Product Interoperability Challenges

Most of the current identity management products and solutions rely on self-contained, standalone management and control tools. Little integration or interoperability is available with other management tools to deal with the management of security, trust, and privacy in an orchestrated way. To react to changes, identity management products and solutions need to evolve toward higher levels of interoperability, flexibility, and capability.

Summary of Identity Management Concepts

From a technological and IT perspective, identity management is just one aspect of managing business solutions and the overall IT stack of networks, platforms, OSs, applications, middleware, and services. Identity management must be considered in a holistic way by including the management of security, trust, and privacy along with the management of policies, requirements, and changes. All of these aspects are interrelated and affect business solutions and the IT stack at different levels of abstraction.

The components within the identity management landscape are rapidly changing. Classic identity management components are consolidating. On the other hand, new components and standards are emerging, such as identity federations, identity for web services, and privacy.

Identity management is also gaining importance. Future identity management solutions will play a more central role in the IT industry due to the pervasiveness and the increased presence of identity information in all components of the IT stack.

HP Identity Management Products and Solutions

For HP, identity management is the ability to:

• Identify every user, application, and device throughout and across organizations over time
• Provide flexible authentication, access control, and auditing technologies, while respecting privacy and regulatory controls
• Bring management capabilities to individuals, small organizations, and large organizations via easy-to-use and understandable tools that cope with dynamic populations and business changes

Considering the above definition, HP’s identity management vision is clearly centered on the pervasiveness of identity management technologies and solutions:

• Identity management is about the management of user, application, and device identities.
• Identity management is about the management of identities in different contexts: enterprises, small and medium businesses (SMBs), and consumers.
• Identity management deals with the management of the entire life cycle of identities and their attributes.

The following sections explore the identity management solutions HP provides to build identity management services for IT infrastructures. We will address identity repositories, security components, privacy management, identity life cycle management, and federated identity management. All of these building blocks are fundamental pieces of the solutions rooted in HP’s identity management vision.

Identity Repositories

Directories are the most commonly used repositories for storing identity-related information. As mentioned previously, identity management solutions can incorporate other repositories, including SQL-rooted databases and XML-formatted files.
Types of Directory-Based Identity Repositories

Different technological approaches exist for directory-based identity repositories: centralized enterprise directories, directory synchronization utilities, meta-directories, and virtual directories. Of these, only a centralized enterprise directory is a true identity repository. The other tools integrate and link different identity repositories.

• **Enterprise directories** are a single authoritative source for identity information throughout an enterprise. All users and directory-enabled applications rely on the identities stored in the enterprise directory. This is the ideal scenario. However, most enterprises cannot use this approach due to the presence of legacy directories.

• **Meta-directories** provide a consolidated view of the identity data stored in different repositories. They also synchronize the data in the different repositories. A meta-directory resembles an advanced directory synchronization utility. Most meta-directory solutions come with workflow logic, and they overlap with many of today’s identity provisioning solutions.

• **Directory synchronization utilities** are intelligent LDAP-based utilities that can synchronize identity data between different types of identity repositories—such as directories, databases, and the repositories linked to enterprise resource planning (ERP) systems.

• **Virtual directories**, unlike meta-directories, do not build a central repository. Instead, they rely on directory server or client functions to access the data stored in different directory sources. Virtual directories also allow for the creation of different application-specific views of directory data.

<table>
<thead>
<tr>
<th>Table 2–2</th>
<th>Directory Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vendor</strong></td>
<td><strong>Directory Product</strong></td>
</tr>
<tr>
<td><strong>Enterprise Directory</strong></td>
<td></td>
</tr>
<tr>
<td>Novell</td>
<td>eDirectory</td>
</tr>
<tr>
<td>Microsoft Corporation</td>
<td>Active Directory Application Mode (ADAM)</td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle Internet Directory Server</td>
</tr>
<tr>
<td><strong>Meta-Directory</strong></td>
<td></td>
</tr>
<tr>
<td>Microsoft Corporation</td>
<td>Microsoft Identity Integration Server (MIIS)</td>
</tr>
<tr>
<td>Critical Path, Inc.</td>
<td>Metadirectory Server</td>
</tr>
<tr>
<td>Siemens</td>
<td>DirX</td>
</tr>
<tr>
<td><strong>Directory Synchronization</strong></td>
<td></td>
</tr>
<tr>
<td>HP</td>
<td>LDAP Directory Synchronizer (Compaq LDSU)</td>
</tr>
<tr>
<td>IBM Corporation</td>
<td>IBM Tivoli Directory Integrator</td>
</tr>
<tr>
<td><strong>Virtual Directory</strong></td>
<td></td>
</tr>
</tbody>
</table>

**HP and Identity Repositories**

HP considers directory identity repositories a mature market and uses a best-of-breed and end-user preference approach. Additionally, numerous applications offer LDAP access to their user (identity) tables such as Resource Access Control Facility (RACF) and Lotus Notes. Table 2–2 gives a non-exhaustive overview of directory solutions.
Security Components

This section discusses the triple-A components of an identity management solution: authentication, authorization, and auditing services. It provides details about the solutions HP offers in this space.

Authentication Technologies

Authentication is the process of verifying an entity’s identity. Authorization credentials, which are uniquely linked to an entity, are typically used for verification. The security quality of authentication technologies largely depends on the following dynamics: the number of authentication factors, the authentication protocol, and the authentication method.

Multi-factor authentication methods offer higher security quality than single-factor authentication methods. A good example of a multi-factor authentication system is a smart card. It combines possession (of the card) and knowledge (of the card’s PIN). Table 2–3 gives an overview of different authentication methods and the number of authentication factors they support.

<table>
<thead>
<tr>
<th>Authentication Factor</th>
<th>Password or PIN</th>
<th>Smart Card or Token</th>
<th>Biometric Device</th>
<th>Biometric Device and Smart Card</th>
<th>Dial Back</th>
<th>Trusted Platform Module (TPM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Possession</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometric Data</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Location</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Many identity management solutions require the authentication infrastructure to support multiple authentication methods and protocols. This may be necessary when the environment supports internal and external users that access a variety of resources. When resources hold different values or contain sensitive information, different methods and protocols may also be necessary. Access to confidential information, for example, may require a stronger authentication method than access to information published on a corporate intranet. In some authentication infrastructures, this feature is known as graded authentication. This simply means that the resources and information a user is allowed to access vary depending on the strength of the authentication protocol and method.

Strong Authentication

Today’s problems of identity theft and the misuse of identities and their attributes are accelerated by the ever-increasing amount of interconnected users, applications, and devices. To attain greater levels of authentication, identity management solutions require strong authentication. Over the last decade, strong authentication has been associated with both cryptography- and multi-factor-rooted authentication. Cryptography-based authentication means that the authentication protocol includes cryptographic operations in the identity and credential verification process. Table 2–4 on the following page provides descriptions of popular strong user and device authentication solutions.
<table>
<thead>
<tr>
<th>Strong Authentication Solution</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strong User Authentication</strong></td>
<td>Hardware tokens are liquid-crystal display (LCD) panel devices that display number sequences that change periodically, for example, once per minute. In combination with a PIN, the token’s software uses these sequences to create one-time passwords. Some tokens challenge the user with a built-in numeric keypad to calculate the passwords. Examples are the tokens from RSA (SecurID) and Vasco.</td>
</tr>
<tr>
<td>Smart Card–based Tokens</td>
<td>Smart cards are devices that can take a number of different physical forms. Most smart cards are similar to credit cards, with the addition of small, dime-size memory chips or microprocessors. USB tokens can operate similarly to smart cards, and some vendors have implemented smart card functionality on cell phones and PDAs. Smart cards and other tokens are tamper-resistant devices that can be used for secure storage of private keys, passwords, and other personal information. Some models perform private key operations (generation, signing, and decryption) in a safe, isolated manner on the card itself. Smart card solutions require smart card readers to be deployed or integrated with the devices.</td>
</tr>
<tr>
<td>Software Tokens</td>
<td>Software tokens operate like hardware tokens, except that a software program installed on a user’s workstation or other computing device (PDA or Pocket PC) provides a token generator or challenge/response system.</td>
</tr>
<tr>
<td>Biometric Authentication</td>
<td>Biometric authentication mechanisms match a physical characteristic of a user against a database record. Common methods include retinal, palm, or fingerprint scans, as well as voice authentication. After years of development, these systems are becoming more reliable, yielding fewer false positives and false negatives. Prices are also falling, making biometrics increasingly practical, though still far more expensive than free passwords. Biometric solutions are particularly successful in physical facilities authentication and government applications like border security and law enforcement.</td>
</tr>
<tr>
<td><strong>Strong Device Authentication</strong></td>
<td>Radio Frequency Identification (RFID) An RFID system is a tag, which contains a miniscule computer chip and an antenna, that is attached to or embedded in an item. Items can be anything from a computer, to a dishwasher, to a living being. The tag transmits a signal to an electronic reader, which associates the signal with the specific item to which it is attached. The reader transmits this information to servers that collect and organize the data for tracking. RFID systems have the power to dramatically refashion such processes as the supply chain by making them more efficient, and they can bring direct consumer and societal benefits such as personalized shopping, medical reminders, and the identification of toxins before they reach landfills. However, the potential to tag and track every item raises privacy and civil liberty concerns. RFID technology has the potential to invade customer privacy and diminish customer control over personal information.</td>
</tr>
<tr>
<td>Trusted Platform Module (TPM)</td>
<td>A TPM, also known as a virtual smart card, is uniquely bound to a single computer platform and can be used for both user and device authentication. TPM core components are an RSA engine, a hash engine, a key generator, and a Random Number Generator (RNG).</td>
</tr>
</tbody>
</table>

**HP Strong Authentication Solutions**

HP offers a variety of strong authentication solutions. These include smart card technologies, biometric devices, RFID technologies, and TPM solutions.

HP ProtectTools Smart Card Security Manager is HP’s strong authentication solution rooted on smart cards. It has several unique features:

- Smart card in BIOS allows for pre-boot authentication and is OS independent.
- Smart card logon allows for strong, smart card-based Microsoft Windows authentication without requiring a PKI.

HP ProtectTools Smart Card Security Manager is available on several HP Compaq notebook models. For the current model list, see [www.hp.com/go/notebook](http://www.hp.com/go/notebook).

HP biometric solutions include the HP PCMCIA fingerprint reader and the HP built-in fingerprint reader for the HP iPAQ Pocket PC. For more information about current HP biometric solutions, see [www.hp.com/go/security/identity](http://www.hp.com/go/security/identity).

HP is leveraging its experience, expertise, and understanding of RFID technologies in its consulting services, and is one of the world’s largest players in the space. HP has taken a leadership role in developing RFID standards. In fact, HP was performing trials and pilot projects long before January 2005,
when Wal-Mart and the U.S. Department of Defense insisted that their suppliers begin using RFID tagging. With the world’s ninth largest non-military supply chain, HP wants to demonstrate the value of RFID systems for increasing the end-to-end speed and visibility of supply chains.

HP’s TPM solution is called HP ProtectTools Embedded Security. HP is the co-founder and leader of TPM specification development within the Trusted Computing Group (TCG). (For more information about the TCG, see www.trustedcomputinggroup.org.) HP ProtectTools Embedded Security is now available on many HP computers and notebooks. See www.hp.com/go/security/trusted for a complete list.

**Single Sign-On**

Single sign-on (SSO) is the ability of a user to authenticate once to a single authentication authority, obtain a credential token or artifact with a defined lifespan, and use it to access other protected resources without re-authenticating. The Open Group (www.opengroup.org) defines SSO as the "mechanism whereby a single action of user authentication and authorization can permit a user to access all computers and systems where that user has access permission, without the need to enter multiple passwords."

**HP and Single Sign-On**

HP provides web-based SSO as part of HP OpenView Select Access, a web access-management solution. For enterprise SSO, HP takes a best-of-breed approach, leveraging the solutions from industry leaders such as Passlogix (v-Go SSO; www.passlogix.com) and Citrix Systems (Metaframe Password Manager; www.citrix.com). HP also offers HP ProtectTools Credential Manager, a client-side credential caching SSO solution in the HP ProtectTools suite.

**Authentication Support in HP OpenView Select Access**

HP OpenView Select Access is HP’s web access-management solution. The authentication methods it supports are presented in Table 2–5. Select Access supports at least three strong (two-factor and above) authentication mechanisms. These are: X.509 PKI certificates, RSA SecurID tokens, and Remote Authentication Dial-In User Service (RADIUS) tokens. HP also has considerable experience with building Select Access plug-ins to add support for other third-party strong authentication mechanisms and protocols.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password</td>
<td>User name/password as stored in the user’s Select Access Directory Server record</td>
</tr>
<tr>
<td>Microsoft Windows NT LAN Manager (NTLM)</td>
<td>Microsoft Windows domain authentication for authentication against Microsoft Windows NT, Microsoft Windows 2000, and Microsoft Windows XP domain controllers</td>
</tr>
<tr>
<td>Registration</td>
<td>Allows users to self-register to Select Access, resulting in a user record in the Select Access Directory Server</td>
</tr>
<tr>
<td>Security Assertions Markup Language (SAML)</td>
<td>XML standard allowing for the transfer of credentials (security assertions) between two authentication and authorization infrastructures, which allows controlled, trusted access between federated entities</td>
</tr>
<tr>
<td>Integrated Windows</td>
<td>Allows single sign-on to web-based applications through Microsoft Internet Explorer and Microsoft IIS from the desktop login, with no re-authentication required</td>
</tr>
<tr>
<td>SecureID</td>
<td>Support for RSA SecurID 2-factor token authentication</td>
</tr>
<tr>
<td>Remote Authentication Dial-In User Service (RADIUS)</td>
<td>Support for token solutions using the RADIUS challenge/response mechanism</td>
</tr>
<tr>
<td>Certificate</td>
<td>X.509 PKI certificate authentication using smart cards, cryptographic tokens, or certificates embedded in the browser, through client-side SSL authentication</td>
</tr>
<tr>
<td>Kerberos</td>
<td>Support for authentication against Microsoft Windows 2000 domain controllers</td>
</tr>
</tbody>
</table>
The Select Access Policy Builder, a security policy management interface, allows for centralized administration of passwords and authentication policies. Password policy data is stored in the directory server. The Policy Builder supports two levels of password policy management: organization-wide policies and individual user preferences. Select Access provides the ability to define strong password policies, significantly increasing the security of password-based authentication.

Select Access supports native password management capabilities including password strength characteristics (length, detection of user name match, dictionary match, and password history), expiry policies, and account lockout based on suspicious behavior. Administrators can define expiration periods for users to change their passwords. They can also set temporary passwords for new accounts, forcing users to select a new password on first login.

Authorization Technologies

The goal of an authorization system is to protect resources and information while allowing fluid access for legitimate users of these resources. Authorization is the act of granting subjects access rights to protected resources. The main difficulty is scaling authorization policy administration to thousands—possibly millions—of subjects and protected resources. As the numbers grow, administrators need to reduce the ratio of policies to the number of subjects and protected resources without compromising the security of the system.

Authorization policies are rules for determining which subjects are allowed to access resources. In some cases, privacy considerations may require support for some form of anonymous or pseudonymous access. In most cases, however, users must be identified prior to receiving the authorization to access resources. An identity management infrastructure is therefore critical to establishing users' identities as the basis for authorizing access to resources.

Two interesting access-control models used in the identity management infrastructure are the role based access control (RBAC) model and the rule set based access control (RSBAC) model. A role is an organizational job function with a clear definition of inherent responsibility and authority (permissions). The process by which an enterprise develops, applies, and maintains RBAC is known as role engineering. As old roles are retired or modified and new roles are defined to meet changing business needs, an enterprise defines processes for updating roles.

Role-based approaches are suitable when job functions are easily partitioned. Wide-scale implementations remain stalled because of the complex nature and large scope of role engineering projects, transitory job assignments in knowledge-based organizations, lack of funding, limited standardization, and proprietary access control mechanisms. A common challenge facing role-based systems is finding agreement among stakeholders for standardized vocabularies and role definitions.

An alternative to an RBAC approach is RSBAC. Most web access-management products adopt RSBAC, including HP OpenView Select Access. With this approach, access is granted or denied based on a set of pre-defined rules or organizational policies. Access control decisions can change dynamically based on access control policies. Rules are context dependent: they can take into account things like the time of day, resource type, and access location.

Authorization Support in HP OpenView Select Access

Web access-management products like HP OpenView Select Access typically combine basic RBAC support (with limited hierarchy and constraint capabilities) and RSBAC support.

With its matrix-based representation of users and resources, HP OpenView Select Access Policy Builder simplifies the complicated and often time-consuming process of creating and applying authorization policies. With simple visual icons and inheritance rules, the Policy Builder makes policy logic easy to
understand. This reduces the amount of errors typically incurred by other list-based access management systems. Beyond simple allow and deny authorization policies attached to each matrix intersection, the Policy Builder allows for further control with conditional access rules.

Auditing Technologies

Auditing systems capture security-related events in identity management systems and ensure accountability for the underlying IT and security infrastructure. Complete and accurate audit and event records provide the evidence that enterprises need to demonstrate compliance with business, security, legal, and regulatory mandates. It is especially critical to audit the authorization, provisioning, and privacy components of identity management systems, which may create or remove user privileges and accounts.

HP OpenView Select Access Secure Audit Server

The HP OpenView Select Access Secure Audit Server provides a consolidated security logging and audit trail. All access requests, authorization decisions, and administrative changes are logged and can be digitally signed to prevent tampering of audit data.

The Secure Audit Server outputs to multiple destinations including databases, e-mail messages, UNIX® syslog, Microsoft Windows Event Logs, and files. Different output destinations can be configured based on the type of audit data, such as audit component and event level (for example, information and warning). All components can store logs and audit information locally in addition to forwarding them to centralized secure audit servers or databases.

HP Select Access by default gathers audit information within all its server components and policy enforcer plug-ins located on the web/application server platforms. This information is a complete record of all transactions within a given Select Access component. Select Access natively stores audit logs and system logs in an ASCII text file using an XML format.

The Secure Audit Server can log information centrally or forward it to any of the supported repositories. It can also make this information tamper-proof by applying digital signatures to the audit trail. Customers have utilized this technique to consolidate audit information from a number of sources.

A Report Viewer interprets the output log files and audit databases collected by the Secure Audit Server. HP Select Access Secure Audit Servers can also send audit information alerts via e-mail to administrators. This can be tied into Simple Network Management Protocol (SNMP) tools through e-mail to SNMP gateways.

Privacy Management

In the context of electronic privacy, users express concerns regarding today’s IT systems and environments like the Internet. Some of the key privacy concerns include:

• Data is collected silently. This is facilitated by the web, which allows large quantities of data to be collected inexpensively and unobtrusively.

• Data from multiple sources may be merged. Non-identifiable information can become identifiable when merged with other sources and information.

• Data collected for business purposes may be used in civil and criminal proceedings.

• Data collected for business purposes may be forwarded to third parties, without notifying the user.

• Users are not given meaningful choices for the use of their personal data.
Privacy considerations typically arise when an organization needs to collect and store customer, employee, and other private data. Other situations that raise privacy concerns include demonstrating conformance with privacy regulations and forwarding user information (identity information, web-service access information, security assertions, or localization data) to third-party service providers.

Numerous efforts have produced legislative frameworks for privacy. Examples are the EU Directive on Data Protection, U.S. laws such as HIPAA and the Children’s Online Privacy Protection Act (COPPA), and frameworks such as Safe Harbor. However, privacy and data protection laws are hard to enforce when personal information spreads across boundaries. In general, users have little understanding or knowledge of privacy laws and their implications. For additional information, see www.privacyinternational.org/survey/phr2003.

Privacy management in an IT environment has many different aspects. These include negotiation, policy life cycle management, enforcement, monitoring, decision support, violation detection, preserving computation, data minimization and transformation, rating and branding, verification and certification, auditing and accountability, mediation and delegation, anonymization and pseudonymization, and user training. In the context of identity management solutions, privacy-protecting technologies can be viewed as an extension to authorization systems. Authorization policies control data access based on factors like privacy regulations and user consent.

Privacy management is an identity management area that requires much work and effort. HP and other major IT players like IBM are leading key developments in the privacy management space. HP is involved in several cross-industry and government-driven privacy standardization initiatives.

"Privacy isn't just about hiding things. It's about self-possession, autonomy, and integrity. As we move into the computerized world of the twenty-first century, privacy will be one of our most important civil rights. . . It's the right of people to control what details about their lives stay inside their own houses and what leaks to the outside."

—Simson Garfinkel, Database Nation
Identity Life Cycle Management

Provisioning solutions are similar to SSO solutions in that they operate from the top down; the application manages all of the systems under it. Administrative functions—from the essential add, modify, and delete to the more general maintenance and monitoring—are under the control of the provisioning system. Provisioning functions can also include non-electronic tasks such as identifying a cubicle, connecting a network port, and acquiring a PC.

With provisioning products, organizations risk implementing one solution that can potentially clash with another. Provisioning solutions often incorporate other parts of the identity management framework, such as self-service and password management.

The only mature provisioning-specific standard at this time is the Service Provisioning Markup Language (SPML). SPML messages facilitate the creation, modification, activation, suspension, enablement, and deletion of identity-related data in different identity repositories. The Organization for the Advancement of Structured Information Standards (OASIS) has been working on the SPML specification since late 2001. For more information, see www.oasis-open.org/home/index.php.

HP OpenView Select Identity

HP OpenView Select Identity is a scalable solution for managing identity within and between large enterprises. The Select Identity solution automates the process of provisioning, managing, and terminating user accounts and access privileges across platforms, applications, and corporate boundaries.

The key features of the Select Identity system include:

- **Business-process aligned management** easily and rapidly manages business or technology changes at micro or macro levels within the managed environment.
- **Centralized management** provides a single point of control for the management of users and entitlements.
- **Provisioning** automates creating, updating, and deleting accounts and entitlements on information systems across the enterprise.
- **Administrative delegation** enables administrative rights to be distributed among multiple tiers of functional departments, customers, and partners.
- **User self-service** enables end users to initiate access to services, change passwords, set password hints, and update general identity information through a simple web browser interface.
- **Approval workflow** automates approval processes required for granting access privileges to users.
- **Password and profile management** manages and distributes password and user profile information across and between enterprise information systems.
- **Auditing and reporting** provides standardized reporting on actions and user account activity.
- **Fully scalable and resilient operation** facilitates today’s global, 24x7 businesses.

Select Identity Architecture

Select Identity is an event-driven, Java 2 Enterprise Edition (J2EE) application that enables clustering, failover, multi-phase commit, and asynchronous operation. All requests to and from the system use HTTP.

Leveraging an open-standard, J2EE Connector Architecture (JCA) bus, Select Identity uses predefined connectors to access backend system data stores. Custom connectors can be readily created, and Select Identity offers a software development kit (SDK) for this purpose. For an up-to-date list of the currently supported connectors, see www.openview.hp.com.
Identity Management With Select Access and Select Identity

Together, Select Access and Select Identity provide a complete answer to complex organizational identity management needs:

- Complete user provisioning for internal and external users
- Easy to manage access and authorization for complex business rules
- Identity life-cycle management, to ensure no lost or forgotten users
- Full-featured user self-service, which cuts the costs of administration
- Multi-step approval workflow ensures the correct authorities are granted
- Profile and password synchronization simplify the user experience
- Password management and self-reset make it easier for users and call desks
- Business process modeling matches the business need
- Full delegated authority provides control where it should be
- Single sign-on aids staff productivity
- Account terminations ensure effective security
- Audit and reporting ensure demonstrable compliance

Federated Identity Management

Federation enables the trusted interchange of security-related information between different autonomous policy domains. Security-related information includes authentication, authorization, and auditing data. Although federation is generally used in the context of an inter-enterprise security mechanism, it can also be used within an enterprise to provide tighter integration between loosely coupled ecosystems.

Typically, a federation provides a common framework for trust—a standard syntax, vocabulary, attribute set, and set of policies and practices for the trusted interchange of security-related information. Bilateral (federation) agreements between partners are often required to negotiate the specifics of access, such as which users or systems can access which resources, under what circumstances, and under what contractual relationships. Access control always remains with the owner of the resource. A federation might also define minimum acceptable trust levels or authentication mechanisms required for specific circumstances.

A federation agreement always deals with two entities: an asserting party that generates security assertions and a relying party that trusts the security assertion made by the asserting party. There are a number of federations being formed, supporting a variety of vertical marketplaces, communities of interest (financial services, health sciences, research and education), and geo-political boundaries (state and national governments).

A variety of standards, specifications, and protocols relate to federated identity management. Figure 2–5 shows the positioning of some of the relevant federated identity management standards. The Liberty Alliance specifications define the protocol messages, profiles, and processing rules for identity federation and management. They rely heavily on other standards such as SAML and WS-Security. Additionally, the Liberty Alliance has contributed portions of its specification to the technical committee working on SAML. More information is available from www.projectliberty.org. HP endorses the Liberty Alliance and actively participates in the creation of its specifications.
SAML is an OASIS specification that provides a set of XML and Simple Object Application Protocol (SOAP)-based services, protocols, and formats for exchanging authentication and authorization information. Currently, work is under way for SAML version 2.0. More information is available from www.oasis-open.org/committees/tc_home.php?wg_abbrev=security.

WS-Security is another OASIS specification that defines mechanisms implemented in SOAP headers. These mechanisms are designed to enhance SOAP messaging by providing a quality of protection through message integrity, message confidentiality, and single message authentication. More information is available from www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss.


Other identity management enabling standards are:

- XML Key Management Specification (XKMS), www.xmltrustcenter.org/xkms/index.htm
- XML Signature, www.w3.org/Signature
- XML Encryption, www.w3.org/Encryption

HP and Federation

HP OpenView Select Federation allows secure and quick extension of enterprises to business partners by enabling rapid integration between different identity systems within and across corporate boundaries. Using industry standard federation protocols, Select Federation links multiple accounts with different providers on the Internet so that secure authentication occurs once per session. Select Federation also enables service providers to offer secure, mobile federated identity services for sharing distributed identity information while protecting the privacy of service consumers.

HP OpenView Select Federation is a protocol-neutral and vendor-neutral solution. It currently supports the Liberty Alliance and SAML protocols, and it will support the WS-Federation protocols when they are ratified. It can also integrate with any vendor’s identity management solution, allowing organizations to protect their investment without worrying about which protocol or vendor to choose for the future.

Select Federation currently supports the following federation protocols:

- SAML 1.0 and SAML 1.1
- Liberty ID-WSF (Liberty Alliance Certified Interoperable)
- Liberty ID-PP (Personal Profile Service)
- Liberty ID-EP (Employee Profile Service)
- Liberty ID-FF 1.2 (Liberty Alliance Certified Interoperable)
- Liberty ID-FF 1.1 (Liberty Alliance Certified Interoperable)
- Liberty LECP (Liberty Alliance Certified Interoperable)
- WS-Security

## Identity Management Summary

Identity management is the ability to identify every user, application, or device across organizations and provide flexible authentication, access control, and auditing while respecting privacy and regulatory controls. Delivered via a set of processes and tools for creating, maintaining, and terminating a digital identity, these tools allow administrators to manage large populations of users, applications, and systems quickly and easily. They allow selective assignment of roles and privileges, making it easier to comply with regulatory controls and contribute to privacy-sensitive access controls.

For HP, identity management is centered on the pervasiveness of identity management technologies and solutions:

- Identity management is about the management of user, application, and device identities.
- Identity management is about the management of identities in different contexts: enterprises, SMBs, and consumers.
- Identity management deals with the management of the entire life cycle of identities and their attributes.

### Table 2–6

<table>
<thead>
<tr>
<th>Solution</th>
<th>IDM Focus Area</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP ProtectTools Smart Card Security Manager</td>
<td>Strong user and device authentication</td>
<td><a href="http://www.hp.com/go/security">www.hp.com/go/security</a> Click HP ProtectTools for Microsoft Products (under Featured Products and Services)</td>
</tr>
<tr>
<td>HP OpenView Select Access</td>
<td>Web access management and web single sign-on</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP OpenView Select Identity</td>
<td>Identity provisioning</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP OpenView Select Federation</td>
<td>Federation</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP Identity Management Services</td>
<td>IDM Consulting and Integration, IDM Managed Service</td>
<td><a href="http://www.hp.com/go/security">www.hp.com/go/security</a> Click Security Services (under Featured Products and Services)</td>
</tr>
</tbody>
</table>
Chapter 3 Proactive Security Management

“IT infrastructures often have inconsistent levels of protection and are prone to experiencing significant negative impacts during security incidents. It is essential to have a holistic and integrated security infrastructure and set of capabilities. This helps to ensure coordinated and consistent levels of protection, enhanced visibility to evolving risks, and effective risk management.”

—Gilles Bouchard, HP CIO and EVP of Global Operations
Proactive security management is an important and integral part of an organization's IT infrastructure management and operations. This key component of HP's security framework focuses on the management of security functions in support of business and organizational goals and processes. The objective is to make sure that the mechanisms for protection are operating appropriately during the setup, operation, and decommissioning of various IT services and assets. Proactive security management also ensures that protection is robust, scalable, and flexible enough to rapidly address changing conditions.

Figure 3–1
Proactive Security Management

In this chapter, we define proactive security management, review the conditions driving its need, and present HP's framework of technologies and services for proactive security management.

Definition

Proactive security management focuses on managing security functions in support of business and organizational goals and processes. It has four distinct attributes that comprise the bigger picture:

- Managing the protection of data, applications, systems, and networks, both proactively and reactively
- Supporting changes to business and organizational models and responding to a changing-threat environment
- Integrating with IT infrastructure management and operations
- Maintaining a level of security and operational risk as defined by the organization

Managing Protection Proactively and Reactively

The fundamental purpose of security products and software systems is the protection of IT assets. In this security context, protection means providing appropriate confidentiality, integrity, and availability for a set of IT assets. Therefore, proactive security management's primary responsibility is to maintain a specified level of confidentiality, integrity, and availability of data, applications, systems, networks, and other IT resources.

With the frequent success of fast and sophisticated attacks, it is apparent that reactive security methods alone are not sufficient. Reactive mechanisms deal with attacks or viruses once they enter the infrastructure—when damage and costs are already adding up. Proactive security management adds
methods, technologies, and services that focus on fixing vulnerabilities before an attack can exploit them. Preventing a security breach makes it easier to maintain business functions compared to when a business is recovering from a successful attack. Prevention is accomplished through the ongoing management of threats and vulnerabilities to the IT infrastructure.

Responding to Changing Business Models and Threats

Once a security infrastructure is in place, it must have the ability to adapt to changes in business models and the various threats that emerge. Business model changes can come from organizational changes such as reorganizations or mergers. For example, the requirements of proactive security management during a merger might include integrating different security technologies like intrusion prevention systems, and managing employee privilege and authority changes. These transitions must happen quickly, and security management capabilities must be efficient.

The threat of attack from criminals, insiders, worms, and viruses is much more unpredictable than changing business models, and the threat environment has shown an increase in the speed and complexity of attacks. The implications for proactive security management include the need for capabilities that can integrate new security technologies and tightly link them with asset, patch, and configuration management systems.

Integrating With IT Management

Distinct security technologies and processes are specific to IT security. These include functional security technologies such as authentication methods (for example, passwords, tokens, and biometrics), encryption methods and encryption key management systems, and firewall systems. Along with security technologies, a number of IT technologies and processes play a significant role in the total security management picture. For example, proactive security management depends on IT workflow systems, trouble ticketing systems, and patch management systems (for testing and applying security-related patches). Having a security operations center that is separate from a network operations center can lead to security decisions that are made without regard to business impact. For example, what if a security decision shut down a vulnerable server that the network operations people were using to handle overflow order traffic? Proactive security management impacts and depends on IT management.

Maintaining Acceptable Security and Risk Levels

Perfect security is an impossibility, and experts recommend spending only as much money as necessary to obtain the appropriate level of protection. The common question is, How much security is enough? The answer is: it depends. It depends on the result of a risk calculation that factors in the value of the protected assets, the threats against those assets, and the vulnerabilities. Security management, in one sense, becomes a tool for managing risk. Maintaining an acceptable level of risk is the highest-level business goal for proactive security management. The acceptable level of risk, however, varies for industries, organizations, and companies, and a functional proactive security management solution provides the correct levels of confidentiality, integrity, and availability to meet the acceptable level of risk.

Purpose

The purpose of proactive security management is to protect assets, enable business processes, and drive costs down. The factors that drive the need for proactive security management include:

- Protecting against increasing threats
- Enabling changing trust models
- Combating increasing process complexity and related expense
- Complying with changing regulations
Protecting Against Increasing Threats

The threat environment is increasingly complex and rapidly evolving. Reports of security incidents are rising, viruses and other attacks are spreading at faster rates, the complexity of attacks is ever more sophisticated, and relatively sophisticated tools for unsophisticated attackers (so-called "script kiddies") are widely available. This environment leads to a number of security management challenges.

As the number and type of incidents increases, distinct protection technologies to prevent new attacks are deployed—for example, firewalls, anti-virus tools, and intrusion detection systems (IDSs). Each new protection technology or component introduces additional complexity in the organization. Each new component must be managed and integrated with the other security protection technologies deployed in the environment. This complexity represents a threat to the security of the organization.

The increasing speed of attacks drives the need for a well-developed incident management program. When attacks operate at computer speed rather than human-scale speed—that is, milliseconds rather than hours—it is necessary to automate responses rather than contemplate actions. This move to a proactive posture of security management also applies to underlying security enforcement technologies; they must evolve to take proactive steps to protect against new, imminent attacks.

To balance security technology, people and processes must not be overlooked. Awareness and training are essential. The more end users can learn about the actions they can and must take to mitigate threats, the more secure the enterprise will become. And the more that the enterprise can capture, learn from, and reuse (as appropriate) best practices in response to threats and attacks, the more efficient the process will become. Unknowing actions can undermine the best-managed security infrastructure.

Enabling Changing Trust Models

The opening of business and organizational boundaries has changed old security models. With any combination of partnerships, mergers, dynamic supply chains, online customer services, federations, and changing user populations, it is very difficult to draw a line showing where an organization’s intranet stops and the Internet begins. The old concepts of inside (people inside the organization—employees or contractors) and outside (everyone else) no longer hold. The reports of incidents involving insiders show that this old, single-wall model of security is not adequate. Proactive security management must now protect a larger set of users that change over time, including a changing set of privileges based on roles, and a set of resources that can expand and contract. This protection must match the speed of the changes. For example, when an employee is hired or fired, access to resources must be disabled in a reasonably short time.

Combating Increased Process Complexity and Expense

New types of attacks cause companies to deploy a growing number of security technologies. For example, a corporate perimeter might use firewalls, routers, and gateways—each with a complex set of rules to create and modify. Behind that might be some bastion hosts, which are server class machines that provide Internet services. Other components of a company’s IT infrastructure might include an IDS, an anti-virus program, and a security patch management system.

From this quick example, the complexity of managing security technologies becomes apparent. Correlating alarms and alerts, consolidating control, centralizing the reporting and management of the entire security operation, and developing in-house expertise for each of these components are significant challenges. Proactive security management solutions and services can simplify or completely offload (if outsourced) the burden of this complexity.
Complying With Changing Regulations

Problems with privacy and lack of security have had enough press and public attention to induce widespread and far-reaching changes in the way we interact with governments, businesses, and organizations. Legislative organizations, standards bodies, and industry-specific groups have created laws, standards, and certifications to guide or mandate how we create, store, use, and communicate information.

In the U.S., for example, the Sarbanes-Oxley regulation requires public companies to show that they preserve the integrity of corporate financial information and take steps to protect that information from unauthorized access. Another U.S. example is the Health Insurance Portability and Accountability Act (HIPAA), which requires enterprises to take meaningful steps to preserve the confidentiality of customer/patient information. Controls such as these drive the functionality of the security infrastructure and require proof of compliance by methods of auditing and event logs.

Proactive Security Management Framework

Proactive security management is comprised of three subcategories:

- Security management processes
- Security management tools
- Enabling technologies

Security Management Processes

Simply having technology and tools does not ensure proactive security management. A combination of people, procedures, and technologies is required to fully implement a proactive security management system. Although most companies recognize the importance of preventing and managing information security incidents, many have limited knowledge of how to do this effectively. And few companies have designed and implemented incident prevention and management processes. This results in companies responding reactively to incidents and losing millions of dollars each year in cleanup efforts. Awareness and training are important security tools. Capturing and documenting best practices helps to continually improve capabilities and avoid security incidents—or at least respond effectively to them.

Security Management Tools

Certain tools make proactive security management more effective, more efficient, and less complex. Critical tasks for these tools include gathering and correlating security events; coordinating and automating responses to attacks; monitoring, testing, and managing patch and update status; prioritizing vulnerabilities and responses based on the scale of the threat; and linking to business objectives.

Gathering and Correlating Security Events

Ideally, management tools collect and report faults from a wide range of subsystems in a centralized fashion. Effective reporting, however, can generate a lot of information. Event filtering tools help system administrators focus on the critical issues.

To be most effective, the tools not only report on specific incidents, but also on broader usage and trends. For example, information from several devices may not reach the alarm threshold for each device, but the information might expose a blended attack or an attack that is trying to remain undetected. Correlating information from different devices assists administrators with finding root causes, determining effects, and making efficient decisions.
Coordinating and Automating Response to Attacks

Given the increasing speed of attacks, automation is often necessary to respond in an appropriate time-frame. Proactive management tools automate responses to security problems, which decreases reaction times and limits the spread of damage. Coordination between security management tools and other IT infrastructure tools adds automation to the process of remediation (fixing vulnerabilities). For example, automatic trouble ticket generation for detected vulnerabilities can create an automated workflow that drives remediation with a manageable, auditable process.

Linking to Business Objectives

Security management tools must link security problems directly to those business processes or services they may affect, so that actions are in line with broader business objectives. For example, a decision to remove a vulnerable system from the network might be delayed while a month-end close is completed.

Enabling Technologies

Enabling technologies provide the underlying technical capabilities to deliver security management and process functionality. They also return feedback information such as auditing and logging data. Enabling technologies are complementary to but different from trusted infrastructure security technologies such as firewalls or IDSs. In this context of proactive security management, the term, enabling technologies is specifically focused on security management and the support of security management processes.

Enabling technologies for proactive security management add capabilities for smarter devices to react automatically in the face of attack. They create new tools for IT and information security organizations to take specific, measured action in the face of imminent attacks before they occur.

HP Proactive Security Management Products and Solutions

The combination of security management processes, security management tools, and enabling technologies comprise HP’s Proactive Security Management strategy. The objective of this part of HP’s security framework is to deliver both the capabilities and the services that help organizations meet the demands of managing the security infrastructure in concert with the overall IT infrastructure.

The security infrastructure is primarily responsible for protecting critical infrastructure and assets. This is the key objective of HP’s Proactive Security Management solutions and services, but it is not a static destination. The strategy also evolves to defend organizations from the increasing threat environment and to adapt to changing trust environments as an organization expands and grows new business models.

HP’s Proactive Security Management products and services integrate with the larger IT management infrastructure, and they perform in a policy-compliant manner that can be audited and proven. HP builds all of its solutions and services with a core design of efficiency and simplicity. Proactive security management reduces the complexity of disparate security functions, infuses technology into devices and systems to make them capable of protecting themselves, and simplifies tasks with automation and policy-based control.

As shown in Figure 3–2, HP Proactive Security Management products and solutions include management programs for security incidents, security events, and security patches. In addition, HP offers an active countermeasures product in the enabling technologies category.

The following information briefly defines these tools, processes, technologies. A detailed description of each area, with specifics such as objectives and benefits, is provided in the sections that follow.
• **Security Incident Management Program** is a set of consulting services that help create and configure processes and tools for managing security incidents throughout their life cycle. It is tailored to the specific business and infrastructure needs of the organization.

• **Security Event Management** is an integrated solution that views, correlates, and manages security events.

• **Security Patch Management** links to the overall incident management process to ensure remediation of security vulnerabilities via patches.

• **Active Countermeasures** is an enabling technology and service capability that proactively mitigates high-risk security vulnerabilities.

**Security Incident Management Program**

A security incident represents an event outside the standard operation of a service that might force an interruption or disruption in the integrity or operation of an IT system. Security incident management is the process that detects actual or potential security incidents and provides resources for resolving the problem as quickly as possible. The process ensures that security incidents are owned, tracked, and monitored throughout their life cycle.

**Objective**

The objective of security incident management is to minimize the business impact of information security incidents by providing timely incident resolution. Initially, it should attempt to prevent security incidents from occurring. For those incidents that do occur, security incident management should:

• Restore normal service quickly and efficiently, with as little impact to the organization as possible

• Ensure that all security incidents are identified and processed in a timely and consistent manner

• Prioritize and provide direct support services where they are needed most

• Provide accurate information about the security incidents that occur to better plan and optimize existing security systems

• Identify, address, and correct or minimize any damage to systems or data

• Evaluate the effectiveness of response(s) and feed a knowledge management system (if available) to learn what worked well and what did not
Benefits

With a comprehensive security incident management program in place, organizations can:

- Minimize downtime, exposure, and loss of critical information caused by actual and attempted security attacks, thereby minimizing damage to business, company brand, customer loyalty, intellectual property, and employee productivity
- Make fast, accurate, reliable, and repeatable security incident and crisis management decisions based on real-time assessments of threats and vulnerabilities, with an associated audit trail and action record to validate proper response and derive improvements
- Prevent or minimize the spread of security attacks within the enterprise and stop the propagation of worms, viruses, and other pathogens to others
- Control internal information for compliance with regulations (for example, Sarbanes-Oxley and the Basel II Accord) and prevent liabilities under the regulatory mandates
- Focus on business rather than security incident recovery
- Control security investments by focusing on the business impact of threats and vulnerabilities

Barriers

Minimizing downtime from security incidents requires a comprehensive security incident response plan to deal with threats that have proven to be very real and costly. Yet few enterprises have such a program in place. Why? HP has found several real and perceived barriers. The most important barriers are:

- **A security staff out of bandwidth** is already over tasked with the mundane. The staff may also lack basic security automation tools such as patch management, group policy, configuration control, and intrusion detection.
- **Missing or poor coordination** across business units, enterprise application owners, data centers, and help desks. Fractured budget and investment policies discourage global, enterprise-wide investment in favor of local quick fixes. These practices result in an overlapping patchwork of solutions that cannot be correlated.
- **The lack of a security governance model** for prompt incident response decisions, making an analysis of the return on investment almost impossible to formulate and justify.

With the cost of the damage caused by viruses and worms estimated at USD $140B in 2003, can any enterprise afford not to have a security incident management program in place?

Defining Information Security Incidents

An enterprise developing a security incident management program must first define an information security incident. Any security incident at any level that threatens a company’s IT infrastructure falls within the scope of security incident management. Examples (in decreasing severity) include:

- A successful compromise or attack upon a system, device, network, application, or associated data. This category includes web server defacements, denial-of-service attacks, account break-ins, system intrusions (with or without immediately apparent harm), loss or compromise of data or other intellectual property, and exposure or deletion of enterprise data.
- A security incident that discloses or risks disclosing sensitive company or customer information to unauthorized parties (such as competitors or the media) and that requires immediate attention to prevent further harm.
- Security incidents that do not in themselves constitute an attack or cause harm but indicate an attempt or a probing effort to find infrastructure vulnerabilities. Security incidents of hostile/unapproved vulnerability scanning (both from within the network as well as from the outside) fall into this category.
• Security incidents that are probably minor, but should nevertheless drive corrective action. Examples here are repeated login attempts, which could be as serious as a dictionary attack or as harmless as an employee who has forgotten his/her password. Other examples are the detection of a rogue wireless access point in the building, which could be an attempt to penetrate the network, a package delivery courier wielding a wireless bar code reader, or an employee simply installing an access point without authorization. (This reemphasizes the importance of user training and adherence to organizational IT security policies.)

HP's Security Incident Management Program

HP’s Security Incident Management Program is a coordinated program of people, processes, tools, and technologies that work together to prevent security incidents and minimize their impact. The HP Security Incident Management Program was designed to reduce the effect of worms, viruses, and related security threats on HP’s own IT infrastructure. For the occasional worm or virus that invades the enterprise infrastructure, no matter how good the defenses are, the HP Security Incident Management Program quickly minimizes the impact.

Key Components

HP has studied the entire security incident process and has identified the key components of a successful security incident management program:

• **Detection and recording.** Before security incidents can be managed, they must be detected. This process initially detects and reports security incidents through a variety of communication vehicles. Security incidents are recorded in order to track, monitor, and update them throughout their life cycle.

• **Classification process.** This process categorizes the security incident and uses impact and urgency information to determine its priority.

• **Investigation and diagnosis.** Investigating a security incident and gathering diagnostic data are drivers for resolving the incident as quickly as possible. This component also allows for incident escalation as appropriate.

• **Major security incident procedures.** HP’s process can identify and immediately flag critical security incidents that require a priority response. While following the normal security incident life cycle, an escalated alarm invokes the major security incident procedure. The procedure stimulates increased coordination, additional communication, and the experienced, knowledgeable resources that high-priority events require.

Elements of HP’s Security Incident Management Program

Any comprehensive security incident management program is built of many sub-components or elements. It is a security-centric view of all activities within the network infrastructure of hardware/devices and the computing infrastructure of applications. The elements include:

• **Threat analysis and response.** Analyzing security threats, assigning severity and criticality for tracking and decision making, and planning the appropriate response and/or remedial action.

• **Vulnerability detection.** Continual vulnerability scanning and probing to identify key, high-risk vulnerabilities.

• **Network intrusion detection and response.** Proactively monitoring Internet-facing infrastructure for signs of network intrusions and other anomalous activities for real-time response.

• **Anti-virus program.** Searching for known and unknown viruses across a heterogeneous IT infrastructure, removing them to help prevent damage, and/or repairing the damaged files left behind.

• **Compliance monitoring.** Monitoring vulnerability patch compliance, security build configuration compliance, security standards compliance, and security regulation compliance.
• **Security monitoring and reporting.** Monitoring configurations and testing for correct patch-level compliance for high-risk vulnerabilities.

• **Active countermeasures.** Conducting regular and targeted scanning for specific, critical vulnerabilities and mitigating risk until systems are patched.

• **Escalation and crisis management.** Managing security incidents, including overall escalation and crisis management, that are anticipated to cause significant impact or have caused enterprise-wide severe impact or interruption.

• **Security incidence response.** Receiving, assessing, responding to, tracking, coordinating, or escalating security incidents to ensure handling of incidents commensurate with their level of risk.

• **Investigations and forensics.** Working with legal, law enforcement, and government authorities to analyze security incident data that involve civil, criminal, administrative, disciplinary, brand, and/or financial implications.

• **Program rollout and awareness.** Developing and delivering end-user and partner-focused communications and awareness activities to increase the understanding of, use of, and compliance with the Security Incident Management Program.

• **Program administration and analysis.** Collecting, consolidating, analyzing, and providing specific audience-based reports to facilitate strategic planning and budgeting.

The above program elements manage the complete life cycle of security incidents—from early threat detection through risk analysis, prevention, remediation, and ongoing protection. By applying a life-cycle approach to security and security incident management, enterprises can prevent and manage information security threats, vulnerabilities, and incidents. In doing this effectively, enterprises minimize the impact of current and future security attacks, and they defend against possible probes and vulnerability scans of the IT infrastructure.

*Figure 3–3*  
HP Security Incident and Event Management Architecture
To support the Security Incident Management Program, HP offers a number of incident and event management products, which are depicted in Figure 3–3 in a high-level architecture. They include solutions for incident response, security monitoring and event management, security reporting, patch management, and vulnerability remediation. HP (along with key partners) completes the picture with security event filtering, aggregation and correlation, policy compliance and vulnerability assessment, and various network security components.

**HP OpenView Service Desk** captures and logs incidents for tracking throughout the security incident management life cycle.

**HP OpenView Operations** provides security event management through integration with key partners for security event filtering, aggregation, and correlation of inputs from various network security components. (These network security components are discussed further in the Trusted Infrastructures Chapter.) Security event reporting is delivered via the HP OpenView Service Information Portal, for a single aggregated view of security incidents.

**HP Active Countermeasures** provides proactive mitigation of vulnerabilities that are deemed high risk via the security incident management program. This protects the corporate infrastructure until security patching or other remediation can be applied. In addition, it provides ongoing monitoring to ensure that these known vulnerabilities are not reintroduced to the infrastructure.

**Security Patching** provides remediation for known software vulnerabilities that lead to security risks for the infrastructure. HP OpenView Radia provides broad patching capabilities, including security patching. HP also offers a vulnerability and patch management solution for HP ProLiant servers as well as specific security-patching solutions for Microsoft® Windows®, HP-UX, and Linux.

These program pieces help to provide the technical infrastructure that supports the overall HP Security Incident Management Program. More details about these solutions are provided in the remainder of this chapter.

**Summary**

The complexity of a best-in-class security incident management program is directly related to the size and complexity of a company’s IT infrastructure, its geographic reach, and its business needs. Many of the functions of an effective security incident management program are combined and owned by a few individuals. However, regardless of how many people are involved, the functions and processes need to be well defined and followed.

HP’s Security Incident Management Program has been very successful. As a testimonial, the same team that helped develop and implement HP’s internal Security Incident Management Program also developed the Security Incident Management Consulting Solution, now offered worldwide. It is important to emphasize that the entire cost of developing and implementing a comprehensive security incident management program can be justified by comparing it to the cost of damage from a single security incident.

**Security Event Management**

Security event management (SEM) is the ability to manage security across the entire IT infrastructure—from systems, applications, network elements, and security devices to all of the communications and transactions occurring within the infrastructure. SEM is a process embodied in the policies, network hardware, and specific SEM applications and services resident in the IT infrastructure. In total, it presents a complete view of the entire range of IT security elements.
Objectives

A comprehensive SEM solution actively records, views, analyzes, and manages all of the security events that occur within enterprise IT infrastructures. SEM includes the correlation of security data from multiple devices and systems across the enterprise to help facilitate security assessments and provide appropriate mitigation strategies and solutions.

An effective SEM solution aligns with the IT infrastructure so that security events can be judged in the context of the associated business risk. The capacity to determine the system’s level of exploitability, an event’s impact on business service, and the weight of assets all contribute to determining the criticality of a potential security incident.

Environment

The major challenge facing the contemporary enterprise goes beyond its own borders and carefully controlled wide-area linkages. Today, enterprises are operating with multiple platform types and security products in an environment that exhibits an ever-widening array of connectivity requirements across partners, customers, and remote offices. Only a centralized view can identify incidents that require remediation and harden enterprise systems against future attacks. A centralized view aggregates all security events—no matter what, when, or where—and intelligently correlates the events with activity patterns.

Evolving government regulations are reinforcing the need for an effective SEM solution within an enterprise. Regulations now mandate organizations to implement security controls, and they hold organizations accountable, both legally and financially, for security incidents that compromise private information. These regulations drive architects and developers of IT security infrastructures to find a solution that constantly monitors networks for vulnerabilities. This has led to a number of toolsets, appliances, devices, and applications of increasing sophistication and scope.

Benefits

The correct SEM solution (properly architected, implemented, and administered) significantly eases the burden on overworked IT and security departments. By quickly identifying and removing security threats and changing from a reactive mode to a proactive, systematic methodology, an SEM solution provides a productivity boost and reduces the direct costs of security implementations over time. The net effect is compliance with government regulations, protection of the corporate bottom line, and smoother business operations.

By integrating a complete solution for SEM with the overall architecture of an incident management program (see Figure 3–3 on previous page) an enterprise is able to:

- Insulate the higher-level incident management processes from the dynamic, ever-changing details of the security profile of a typical enterprise network. A network that is not only heterogeneous (containing a range of technologies, applications, and vendor-specific solutions) but also diverse in geography, time zone, applications, use patterns, and languages down to the operating system level.
- Conduct event filtering at the correct level while retaining sufficient audit and action records to validate any security oversights of critical components and information, if needed for legal or regulatory reasons.

**HP Definition of Security Event Management**

*Security event management (SEM)* is a filtering mechanism that monitors security-related events and transaction activities (collected in log files and by other means) and passes those events representing a security threat or a potential security threat to a higher level for further analysis, correlation, examination, escalation, and reporting, while simultaneously screening out routine events that are compliant with the enterprise security policies and procedures.
• Manage the SEM system from a higher-level perspective and easily adapt the system to changes in local infrastructure and network conditions (granular adaptation) as well as to changes in the overall threat level and profile on the worldwide network (global adaptation).

• Demonstrate due diligence if a regulatory agency investigates the enterprise for compliance or if a legal action related to a security incident arises.

HP's Security Event Management Program

A typical Fortune 1000 company can have thousands of deployments of individual security solutions. These solutions are a combination of hardware and software products that implement functions such as access authorization, identity management, virus detection, intrusion detection/prevention (IDS/IPS), and other security measures. Those responsible for such infrastructures have the dual (and often contradictory) responsibilities of maintaining security while at the same time delivering computing services at predefined levels of performance and availability. Because the former so affects the latter, success comes only through strong, centralized control of solutions coupled with the intelligent management of security events and IT system transactions.

Figure 3–4 highlights the components of HP’s Security Event Management products and solutions within the HP Security Incident and Event Management architecture.

Figure 3–4
HP Security Event Management Components

HP OpenView for Proactive Security Management

An HP OpenView-based SEM solution enables enterprises to detect and dynamically respond to changing circumstances. It also helps to securely manage evolving IT environments, minimizing any operational impact due to security events. Intelligent partner integration, along with the best point solutions, provides an end-to-end global and local security management solution that proactively mitigates security incidents.
Vulnerability assessment, patch management, pre-emptive notification, security incident detection, HP Active Countermeasures, and incident management detect weaknesses before they can be exploited. HP OpenView pulls together all of the localized security partners’ products to provide a single, global view of security events.

HP OpenView Operations (OVO), HP OpenView Network Node Manager (NNM), and HP OpenView Service Desk combine to link the security team to the larger IT department, enabling a cross-functional team that better mitigates risk across the enterprise. HP’s OpenView-based SEM solution provides the technology, tools, and services framework for HP’s Security Incident Management Program.

Detection of a security event can come from multiple sources: IDSs, firewalls, and system log file monitoring and analysis. Preventative notifications of potential security incidents (including unusual usage patterns and unapproved configuration changes) and early warning services can help mitigate incidents before they do damage. HP’s unique Partner Integration Strategy achieves the highest level of integration in the industry through the development of Smart Plug-ins (SPIs) that integrate with HP OVO. SPIs collect and intelligently analyze alerts. They correlate alerts as necessary, and forward them (if appropriate) to a higher level in the management hierarchy. SPIs also monitor the health, performance, and availability of the individual security applications and devices. SPIs are the preferred integration method for linking security devices and applications into OpenView.

HP’s Event Correlation Solutions (ECS) can correlate individual event streams while also correlating events across security, system, application, and network sources. ECS provides the flexible mechanism for rule-based event correlation and processing the real-time event flows. For network-based security management, HP OpenView Network Node Manager provides the industry’s leading Simple Network Management Protocol (SNMP)-based system, including log file monitoring and analysis.

HP’s partner integration strategy achieves the following:

- Unified fault management covering all subsystems, collected and reported in a centralized fashion
- Unified reports covering specific incidents plus broader usage trends
- Event filtering to shield operators from trivial matters, enabling them to focus on the most critical issues
- Event correlation to deduce cause and effect from seemingly dissimilar events
- Automated actions in response to a security problem, such as shutting down a process, paging an operator, generating an incident trouble ticket, or initiating a change management process (for example, to deploy patches)
- True service-level management, where specific security problems are immediately linked to those services they may affect, so actions can be taken in line with broader business objectives

What HP Provides: HP and Partner Solutions

HP OpenView provides a framework on which an enterprise can build a complete security management solution. A best-of-breed global management solution relies upon a collection of point solutions integrated into the OpenView architecture.

Creating the best of both worlds results in effective security management only if local solutions and global management are integrated to act as one. Such integration goes far beyond simply passing events from one application to another. Excellent integration takes full advantage of the local product’s understanding of the managed object, plus the global solution’s understanding of the complete infrastructure.

HP’s approach relies on both internal expertise as well as that of our partners, and it provides enterprises with the ability to select the correct and most effective local solution for their situation.
HP's Partners and HP OpenView


Summary

HP has built a complete solution for an enterprise Security Incident Management Program that is exceptionally robust, sophisticated, and scalable. As a component in managing the Adaptive Enterprise, the HP solution is based on three critical elements:

• The scalable, secure, and proven HP OpenView platform
• A set of underlying data collection and analysis applications, running as SPIs to the HP OpenView platform
• Extensive and sophisticated processes and procedures that tie all components together with a robust and scalable platform and use additional HP OpenView components such as trouble ticket management to provide overall IT service management capabilities

The primary benefit of the HP OpenView approach is that an enterprise can take a holistic view of its entire IT infrastructure over the complete life cycle of the infrastructure’s individual components. As the networks, systems, and applications build and adapt to the changing requirements of the enterprise, so can the HP OpenView solution.

Security Incident Management becomes integrated with the entire organization’s approach to IT and network management. Components (such as firewalls, patch management solutions, and IDSs) that once were islands of individual solutions and tactical approaches to local problems become part of a much more comprehensive solution.

Security Patch Management

Security patch and configuration management incorporates security patches, correct configurations, and current versions of software. Eliminating vulnerabilities before incidents can occur is the greatest defense against attacks. By removing a vulnerability, the threat is instantly and permanently removed.

Objectives

Security patch management solutions should provide quick and reliable automation of the patch management process. Policy-based solutions help managers ensure that systems are current and that the security and stability of systems are optimized. Updating network nodes with the latest security patch is only part of the battle. Knowing what security patches to deploy and when to do so are key parts of any security patch management solution.

Environment

Although the patches are available, their deployment proves to be a challenge to enterprises. There are multiple reasons for this:

• **Frequency of vulnerabilities and patches.** The monthly rate of security vulnerability discovery and posting of patches has risen exponentially over the past few years.

**According to data from the FBI and Carnegie Mellon University, more than 90 percent of all security breaches involve a software vulnerability caused by a missing patch that the IT department already knows about.**

“Five Tips for Effective Patch Management,” Computerworld magazine, July 2003
• **Quality versus speed during patch application.** Testing and qualifying patches to ensure that they will not impact the overall operation of the system has always been a concern. The speed in which security patches need to be deployed make this testing and qualification process particularly challenging.

• **Ability to audit patch implementation.** The ability to audit systems to ensure patch compliance has been an ongoing challenge, especially in diverse multi-operating system environments with desktops, servers, and mobile devices.

• **Number of mobile and remote users.** Additional mobile and remote users bring challenges to an enterprise’s patch capability. Mobile and remote users miss critical notification if they are not connected when an audit or scan takes place. Once notified, they may have limited bandwidth for accessing and installing patches. Finally, they may be exposed more quickly to attacks because they are located outside the protection of the enterprise.

**HP’s Patch Management Programs**

HP Services combines the expertise of Certified Information Systems Security Professionals (CISSPs) and Microsoft Certified System Engineers (MCSEs) to recommend and deploy the right security patch management solution for an organization. Solutions cover a range of operating environments, including Microsoft Windows, Linux, and HP-UX. These solutions include HP OpenView Patch Manager, ProLiant Essentials Vulnerability and Patch Management Pack, Microsoft Security Patch Management tools, and HP-UX Patch Management tools.

**HP OpenView Patch Manager**

HP OpenView Patch Manager using Radia eliminates known software vulnerabilities quickly and reliably by automating the patch management process—including acquisition, impact analysis, pilot testing, discovery, assessment, deployment, maintenance, and compliance assurance—to ensure that devices are configured correctly. Using this policy-based software, IT managers can accelerate the correct configuration of their software infrastructure and optimize the security and stability of managed systems. HP OpenView Patch Manager using Radia provides value for business continuity and security initiatives, server provisioning and repurposing, and OS and application migration.

**ProLiant Essentials Vulnerability and Patch Management Pack**

For more specific security patch management, the ProLiant Essentials Vulnerability and Patch Management Pack integrates comprehensive vulnerability assessment and advanced patch management functions with HP Systems Insight Manager. It identifies and resolves security vulnerabilities quickly, efficiently, and reliably. The Pack can be used independently or integrated with a broader patch management solution like the HP OpenView Patch Manager.

Features of the ProLiant Essentials Vulnerability and Patch Management Pack include:

• **Combined vulnerability assessment and patch management.** Single tool seamlessly combines the assessment and the remediation of vulnerabilities, reducing the operational complexity that arises from managing separate tools.

• **Integration with HP Systems Insight Manager.** Enables use of existing functionality (such as discovery, identification, scheduling, role-based security, notification, and group-based actions) to eliminate the need for users to recreate tasks in multiple tools for vulnerability assessment and patch management.

• **Comprehensive vulnerability assessment.** Coverage of vulnerabilities reported in all leading vulnerability databases ensures comprehensive assessment. Powered by Harris STAT® Scanner (the only Common Criteria Certified scanner, an internationally accepted security qualification), the assessment identifies vulnerabilities reported in the Common Vulnerabilities and Exposures (CVE)
list, the Federal Computer Incident Response Center (FedCIRC) vulnerability catalog, the SANS Top 20 Internet Security Vulnerabilities list, the CERT/CC advisories list, and the U.S. Department of Energy Computer Incident Advisory Capability (CIAC) bulletins.

- **Acquisition, deployment, and enforcement of patches.** Automatically collects new vulnerability updates and patches directly from vendor sources, such as a vendor’s web-based patch depository. Patch manifests, which break down each patch into its component parts, are created automatically.

- **Centralized management.** Schedulable patch deployment, patented differencing (differences between actual and expected configurations), and checkpoint restarts (resuming processes at checkpoints due to interruptions) ensure that patches are deployed with minimal impact on network resources and allow patches to be managed from a central point.

- **Unique desired-state management.** Automatically and continuously ensures that patches remain applied in their proper state. If patches are corrupted in any way, they are automatically reinstalled to bring the system to the desired patch level.

- **Server lifetime coverage.** License provides coverage for the lifetime of the server for software upgrades and vulnerability updates.

### Microsoft Security Patch Management Tools

Microsoft Corporation provides several tools to help with security patch management:

- The **Microsoft Baseline Security Analyzer (MBSA)**
- The **Office Update Inventory Tool**
- **Windows Update, Office Update, and Software Update Services (SUS)**
- **SUS Feature Pack for Systems Management Server (SMS) 2.0 and SMS 2003**

The MBSA tool can perform a general security analysis scan on Windows NT 4.0 and later Windows systems. MBSA also provides patch scanning functionality. In addition, MBSA can be integrated with SUS. This means that MBSA can check the enterprise SUS server for security updates instead of checking the Microsoft Corporation web site. The Office Update Inventory tool is the MBSA equivalent for identifying missing Microsoft Office patches.

The Windows Update web service allows Microsoft Windows 98, Microsoft Windows 2000, Microsoft Windows Me, Microsoft Windows XP, and Microsoft Windows Server 2003 users to easily download and install the latest Microsoft OS patches. It can also be configured to run automatically at predefined intervals. Office Update is the equivalent of Microsoft Windows Update for Microsoft Office patches.

Microsoft has three products for patching and updating: Automatic Updates (AU), the SUS client, and the Microsoft Windows Update Services (WUS) client. SUS builds on the Microsoft Windows Update and AU services. It gives enterprise administrators the ability to provide Windows Update-based security patch services to their users and systems in a controlled and secure manner. SUS can be used to set up an enterprise Microsoft Windows Update server from which internal Microsoft Windows clients can download the latest patches.

The SUS Feature Pack for SMS is Microsoft Corporation’s most advanced security patch management tool. It determines security patch status, distributes patches, installs patches, and generates reports on patch status. It also allows an administrator to identify and target specific computers for security patch updates. The SUS Feature Pack is built specifically for SMS version 2.0 Service Pack 3 or later.

Table 3–1 on the following page provides a summary of Microsoft Corporation patch management tools.
Table 3–1
Microsoft Security Patch Management Tool Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>MBSA</th>
<th>Windows Update</th>
<th>SUS</th>
<th>WUS (beta)</th>
<th>SUS Feature Pack for SMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Security Patch Content</td>
<td>Analysis of missing security patches for the above applications—cannot perform actual distribution and installation</td>
<td>Software updates, critical driver updates, and service packs (SPs)</td>
<td>Software updates, critical driver updates, SPs, and feature packs (FPs)</td>
<td>Software updates, critical driver updates, SPs, FPs for Windows OSs and patches for MS Office, SQL Server, and Exchange Server</td>
<td>Software updates, SPs, FPs and update and application installation of any Windows-based software</td>
</tr>
<tr>
<td>Availability</td>
<td>Free</td>
<td>Free</td>
<td>Free</td>
<td>Free</td>
<td>Based on SMS licensing</td>
</tr>
<tr>
<td>Targeting Content to Systems</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>Simple (based on AD groups, OUs)</td>
<td>Advanced (based on AD groups, OUs, WMI queries)</td>
</tr>
<tr>
<td>Network Bandwidth Optimization</td>
<td>Not applicable</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Patch Installation and Scheduling Flexibility</td>
<td>Not applicable</td>
<td>Manual and end-user controlled</td>
<td>No</td>
<td>Simple</td>
<td>Advanced</td>
</tr>
<tr>
<td>Patch Installation Status Reporting</td>
<td>Not applicable</td>
<td>Install errors and list of missing updates reported to user</td>
<td>No</td>
<td>Simple</td>
<td>Advanced</td>
</tr>
<tr>
<td>Deployment Planning</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>No</td>
<td>Simple</td>
<td>Advanced</td>
</tr>
<tr>
<td>Inventory Management</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>No</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Compliance Checking</td>
<td>Not applicable</td>
<td>Not applicable</td>
<td>No</td>
<td>No, status reporting only</td>
<td>Advanced</td>
</tr>
</tbody>
</table>

HP-UX Patch Management Tools

HP provides a set of tools for managing HP-UX security patch updates in an efficient and effective way. These tools include the Security Patch Check, Bastille, and Install-Time Security.

Security Patch Check (SPC) generates a report of recommended security patches for the HP-UX system and identifies those patches with warnings present. Bastille is an open-source, GNU Public License (GPL) security hardening and lockdown tool. It can be configured to run SPC automatically at regular intervals. This ensures timely identification of new vulnerabilities. Install-Time Security (ITS) verifies that the system is secure by default at installation.

SPC is integrated with ITS to ensure that security patches are current on the server at the time of installation. Bastille can then be set to ensure that SPC runs regularly.

Summary

Security patch management is paramount to maintaining a proactive stance against threats and vulnerabilities. A number of tools available from HP help organizations to manage security independently and effectively across various OSs and platforms. For more effective business continuity and enterprise level protection, security patch management tools can be tied into the larger IT management function via integration with a general patch management tool. In addition, HP’s Security Incident Management
Proactive Security Management

Program identifies and prioritizes critical patches. It conducts system audits to ensure compliance and calculates business risks associated with newly identified vulnerabilities. HP can provide the right level of solution for any business requirement.

Active Countermeasures

Organizations need to be prepared to deal with unpreventable, fast-spreading attacks. Known problems, whether fast or slow, can be prevented. Organizations experiencing slow, unknown problems normally have adequate response time. As Figure 3–5 illustrates, the problem space occurs when an attack is unknown and quick to spread.

Figure 3–5
Matrix for Speed of Attack and Vulnerability Identification

When vulnerabilities are known, tactics such as patches, anti-virus software, perimeter defenses, and scanning can help. On the other hand, slow-spreading attacks can be handled with human-mediated responses, such as generating and distributing threat signatures, monitoring for intrusions, and changing firewall rules. The biggest concern is preventing new, fast-spreading attacks. In most IT environments today, these attacks run rampant until IT staff intervenes. This is where HP can help.

HP has invented a vulnerability scanning and mitigation technology named Active Countermeasures—a powerful tool for identifying and managing vulnerable systems in an enterprise network. HP has employed Active Countermeasures to protect HP’s corporate network since 2002, and the technology has assisted in protecting HP from a number of major Internet worm attacks. Active Countermeasures is an HP patented technology and is available from HP Services.

History

In July of 2001, a destructive worm known as Code Red attacked the Internet. It spread rapidly, caused widespread service delays, and cost millions of dollars due to lost productivity and cleanup efforts. HP, like other major companies, suffered as the worm saturated HP’s worldwide computer networks.

In response to the Code Red attack, a team of HP Labs researchers in the Bristol Trusted Systems Laboratory isolated the Code Red worm, reverse engineered its payload, and then constructed their own countermeasure intended to identify and disable vulnerable systems on HP’s network. HP IT Security, working alongside HP Labs researchers, introduced this countermeasure across HP’s entire corporate network to find and mitigate vulnerable systems.
After proving the effectiveness, scalability, and robustness of the technology, HP IT Security formally adopted Active Countermeasures as part of their Incident Management Program. Now a part of standard processes and procedures, it scans HP’s computer network (which spans some 300,000 network devices) twice a day. Since deployment, Active Countermeasures has dealt with the challenges of the Code Red and NIMDA outbreaks. It also scans and remediates newer vulnerabilities as they become known, such as the Sasser worm.

Technology Overview

Most networks with significant security infrastructure are protected by anti-virus software, intrusion detection technology, and a patch management system. However, these tools are not sufficient to protect against unknown, fast-spreading attacks. Active Countermeasures addresses three common gaps in a security infrastructure that allow the fastest and newest attacks to succeed:

• **Gap 1: Window of vulnerability.** A window of vulnerability exists between the time that an attack or vulnerability is discovered and the time that some kind of mitigation (patch or workaround) is available and installed throughout an enterprise.

• **Gap 2: Unmanaged systems.** Unmanaged systems (for example, contractors’ systems, employees’ home systems, and re-used dormant systems) that connect to the network may not have the latest anti-virus profiles or security patches.

• **Gap 3: Rate of proliferation.** The fastest attacks spread more rapidly than most people, processes, and technologies can respond. (See SQL Slammer sidebar.)

Functions

As shown in Figure 3–6, Active Countermeasures consists of a number of distinct functions and processes. The first function is procedural: observing and researching new vulnerabilities, new exploits, and new dangers in the environment. This is a constant awareness function of gathering information from the

---

**SQL Slammer**

The worm known as SQL Slammer began propagating on the Internet at 0600 hours (GMT) on January 25, 2003. The number of computers it infected doubled every 8.5 seconds in the first minute of the attack. In less than 30 minutes, more than 75,000 computers were impacted worldwide, resulting in business losses estimated at billions of dollars.
Information Sharing and Analysis Center (ISAC), CERT/CC, hacker bulletin boards and web sites, and general knowledge about attacks and vulnerabilities as they arise. The information collected feeds into the second function. The second function is a process of triage: determining the likely effect of a new vulnerability or attack and deciding on the proper response. For many potential attacks, the effect is of low consequence or there is a low probability that the attack will be launched. For these situations, the proper response is to address the potential attack with the current patch management system. However, there are a small percentage of discovered vulnerabilities that represent a high risk to an enterprise. If a new vulnerability is considered to be of sufficiently high risk, a new countermeasure is developed and installed in the Active Countermeasures scanning framework, which is then deployed across the network.

Process

Active Countermeasures tests for a vulnerability by using the same path that a worm might use. If Active Countermeasures can successfully access a target computer using the test, the computer is vulnerable. This technique produces highly accurate results, with no false positives. When Active Countermeasures finds a vulnerable computer, a range of user-defined corrective actions is possible. In many environments, the response could be as simple as a pop-up window informing the system operator to initiate the patch management system at the earliest opportunity.

In certain mission critical contexts, corporate policy may determine that the proper response is to terminate the specific vulnerable application. If the attack is targeting a web server, for example, the right response may be to stop the web server process until the system has been patched. If a mobile employee’s system is going home and coming back into the network, the chosen response may be to simply quarantine the system until it is upgraded with the appropriate set of patches.

Vulnerabilities Addressed

Active Countermeasures is designed to identify and remediate a specific range of high-risk vulnerabilities. The vulnerabilities are those that the most serious worms have exploited, for example:

- **Nimda**, attacks a vulnerable IIS server
- **Code Red**, attacks a vulnerable IIS server
- **Blaster**, attacks a vulnerable Distributed-Component Object Model (DCOM) service
- **Slammer**, attacks a vulnerable SQL server
- **Spida**, attacks SQL servers with known administrator passwords
- **Sasser**, attacks a vulnerable Local Security Authority Subsystem Service (LSASS) process

As new vulnerabilities that satisfy the urgent and high-risk criteria are discovered, new Active Countermeasures are added to this list and released for use.

Summary

Active Countermeasures is a technology developed by HP Labs that has successfully defended HP’s corporate network from a number of critical network attacks since 2002. It has minimized the losses incurred by HP due to business disruption, lost productivity, and cleanup activities. Active Countermeasures was piloted in select HP customer enterprises, and it is now available as a service from HP.

HP Proactive Security Management Services

HP takes a holistic approach to security that includes the people, processes, and technology within our organization to ensure the effectiveness of security solutions. We assist in defining a security strategy specifically tailored to the user’s environment and business processes. HP offers various services at any point in the security management life cycle. With a level of integration that correlates business services
with the supporting infrastructure, HP helps to manage security priorities that are mapped directly to business priorities. HP offers Consulting and Integration Services, Customer Support Services, and Security Services integrated as part of our Managed Services Business.

HP has invested resources to develop comprehensive, effective security services to help ensure the integrity of the computing infrastructure. Our expert security staff includes CISSPs and certified SysAdmin, Audit, Network, Security (SANS) Institute individuals who bring breadth and depth of experience in multi-vendor platforms including HP-UX, IBM AIX, Sun Solaris, Microsoft Windows, and Linux. Our team of experts is backed by an extensive R&D team equipped with the leading-edge tools to investigate and develop countermeasures for the current set of security threats from around the world.

HP covers everything from individual, specific projects (Express Services) to services tailored for those wanting to build a comprehensive security management solution for their business. For more information about HP’s Consulting and Integration Services, Support Services, and Security Services, visit www.hp.com/go/security.

Proactive Security Management Summary

Proactive security management protects data, applications, systems, and networks, both proactively and reactively. It supports changing business and organizational models and responds to a changing-threat environment. Proactive security management focuses on managing security functions in support of business and organizational goals and processes.

HP’s Proactive Security Management products and solutions deliver a set of technologies and services to manage an IT infrastructure’s vulnerabilities, the security infrastructure, and the incidents that occur. The products and solutions integrate with the IT infrastructure and provide a responsive system that can adapt to changes in organizations, business models, and the threat environment. Proactive security management enables the vision of HP’s Adaptive Enterprise by delivering policy-driven security management across the enterprise to prevent, detect, warn about, log, and heal the effects of attacks, security policy violations, and other threats.

Table 3–2
HP Proactive Security Management Solution Offering Summary

<table>
<thead>
<tr>
<th>Solution</th>
<th>PSM Focus Area</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP OpenView Service Desk</td>
<td>Incident response</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP OpenView Operations</td>
<td>Security monitoring</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP Event Correlation Solutions (ECS)</td>
<td>Security event management</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP OpenView Service Information Portal</td>
<td>Security reporting</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP OpenView Patch Manager using Radia</td>
<td>Patch management</td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>ProLiant Essentials Vulnerability and Patch Management Pack</td>
<td></td>
<td><a href="http://www.openview.hp.com">www.openview.hp.com</a></td>
</tr>
<tr>
<td>HP-UX Patch Management Tools</td>
<td></td>
<td><a href="http://www.hp.com/go/unix">www.hp.com/go/unix</a></td>
</tr>
<tr>
<td>HP Active Countermeasures</td>
<td>Vulnerability mitigation</td>
<td>Contact HP for information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click Security Services (under Featured Products and Services)</td>
</tr>
</tbody>
</table>
Chapter 4 Trusted Infrastructure

"Every change in the business triggers an IT event. If you get the infrastructure right, everything is possible."

— Bob Napier, Late CIO, Hewlett-Packard
Today, running a business requires the availability and reliability of the IT infrastructure, which underlies most critical business processes. The reliability of the IT infrastructure is paramount. It implements the appropriate technologies to secure the end-to-end IT infrastructure, including data centers, networks, productivity tools, end-user desktops, and wireless devices. A trusted infrastructure and its network, host, and storage components form the basis of HP’s security framework.

This chapter of the handbook discusses IT infrastructure security across the network, host, and mass storage. It introduces the concepts related to trusted infrastructures, trusted computing, and directions in infrastructure technology. HP’s security strategies for trusted infrastructure are also discussed, followed by detailed information about network, host, and storage security.

**Definition**

Trusted infrastructures are composed of hardware platforms, operating environments, and applications that behave in an expected and predictable way for their intended purpose. Trusted infrastructures support the IT applications underlying critical business processes. When IT infrastructure technologies fail to keep pace with emerging threats, we no longer trust them to sustain the applications we depend on in both business and society.

**Purpose**

The complexity of today’s IT infrastructure opens it to numerous threats. As shown in Figure 4–2, threats and challenges come from a wide variety of sources. These sources range from internal and external attacks to the risks introduced by common requirements for mobility, business partner connectivity, and outsourcing of IT services.

The need for a trusted IT infrastructure flows from an increasing reliance on IT systems to do everything from running businesses to running our society’s utility infrastructures. Just as the dependence on IT permeates all aspects of society, security capabilities must permeate all aspects of the IT infrastructure. Security must be built-in, not bolted-on, at the platform level, at the network level, and in the very processes used for developing systems. A trusted infrastructure reliably manages and controls access to information assets while delivering the horsepower for critical business processes. It helps implement appropriate technologies to secure an organization’s end-to-end IT infrastructure, worldwide.
Initially, security models in computing resembled a fortress with heavily guarded walls. As the power of computing, connectivity, and the Internet has become evident to businesses, this fortress model has shown its limitations. The need for new IT security approaches has emerged as more companies harness the power of the network to do business online with customers and business partners.

Perimeter Security: Keep the Bad Guys Out

In the early days of computing, before its ubiquity in the commercial sector, dependency on IT infrastructures and the need for IT security were strongest for organizations in the government and military sectors. In these contexts, communication security and the need for access control to data were well understood and paramount. Conversely, the commercial sector perceived computing technology as a welcome performance and efficiency improvement—not a necessity. As a result, while computing technology became more widely available, technical developments motivated by the commercial sector focused on usability and performance.

For commercial computing applications, it was initially sufficient for organizational boundaries in the physical world to drive the requirements of mainstream IT security. The focus was on keeping the bad guys out using perimeter security. In the meantime, sensitive government and commercial organizations sought custom solutions to their IT security needs because they could not rely on off-the-shelf commercial technologies.

Many of the architectures that underlie major portions of today’s infrastructures were designed to rely on perimeter security. However, as this perimeter security model has shown its limitations, so have the security models of the computers inside the perimeter.

Trusted Infrastructure: Let the Right People In

In today’s world of remote workers, wireless users, trading partners, and connected customers, the expectations of perimeter defenses must be reexamined. Protecting the perimeter or point of contact with the Internet is still important, but it does not sufficiently provide end-to-end security. An effective security strategy must be far more flexible and sophisticated—simply posting a guard at the gate to the network is not enough. Infrastructure security requirements have evolved from keeping the bad guys out to letting the right people in. Legitimate users should have easy access to authorized resources, but should be prevented from accessing unauthorized resources.
Ongoing Evolution

Organizations continue to use IT in new and changing ways. The evolution in computing and use models initiated by the Internet, connectivity, and mobility is still in its relative infancy. Modern businesses are interconnected with their customers and business partners, and they support an increasingly mobile workforce requiring seamless access to a company’s IT networks from anywhere in the world. Similarly, as IT outsourcing offerings have become more comprehensive, more businesses are choosing a provider to host their IT systems. This recent and widespread evolution of how IT is used to run a business creates new challenges.

Infrastructure Technology Directions

An IT infrastructure is the collection of IT systems supporting a given set of IT applications. The core elements that comprise the fabric of a company’s IT backbone are networking technologies and host technologies. Networking technologies incorporate hardware and infrastructure services and enable the secure and reliable transport of data. By contrast, host technologies incorporate hardware platforms and operating systems (OSs) and enable secure manipulation and storage of data.

Major developments in infrastructure technologies have occurred in the last several years. Mobility is a reality, networking is becoming pervasive, and IT infrastructures are becoming more adaptive and flexible at meeting business needs faster and with lower cost. Important areas of technological development in network security include network security architectures and network-enforced security compliance. Regarding host security, significant areas of development include OSs and hardware platforms.

Network Security Developments

Network Security Architectures

Conventional network perimeter defenses are challenged to simultaneously meet the needs of business agility and information asset protection. For example, firewalls are increasingly managed using exceptions lists, which cause access holes within the firewall. These exceptions result in both security and operational concerns.

An organization cannot afford even one successful penetration of perimeter defenses; an attack jeopardizes the entire data network. In order to retain agility, it is crucial for businesses to manage the increased threat velocity and avoid ad hoc approaches. This has created a strong need for new approaches in the design of data network architectures, which strive to achieve business agility needs while providing security with defense in depth.

Network-Enforced Security Compliance

Today, greater commonality in security functions across Local Area Networks (LANs), Wireless Local Area Networks (WLANs), and Wide Area Networks (WANs) is required. These three types of networks currently exhibit a large disparity in the level of security functions provided by their associated products.

Harmonization of security enforcement is important to help maintain such security policies as access control across the network. It also facilitates central management of the entire infrastructure. Solutions exist today that help to implement such controls above a network infrastructure. However, additional efforts are necessary to provide holistic solutions that effectively deal with complex heterogeneous environments.

Pervasive and manageable security mechanisms are starting to be built into networks, with the help of standards such as IEEE 802.1X (for port-based access control). Additionally, infrastructure protocols such as 802.1X limit access to authenticated devices and users. When combined with a software solution for enforcement of end-point security compliance, these mechanisms help to support security policy
decisions at the network edge. This permits such solutions as quarantining and remediation to take direct action on an authentication or compliance failure. Note also that these approaches are not limited to the network edge—variations often can and should be used in the network core.

Another important development in network security includes the emergence of behavioral approaches to mitigating threats. Building security features directly into the network creates proactive security management solutions. These types of solutions rely on cooperation from the components of the infrastructure for managing and mitigating fast-spreading threats. The Proactive Security Management chapter of this handbook provides details about these emerging solutions.

Host Security Developments

As discussed previously, most businesses now depend on a secure infrastructure. Yet, they deployed platforms and OSs that were not necessarily designed with security requirements in mind, nor were they designed to work together well (if at all) in this regard. As a result, implementers of individual applications have been required to overcome these limitations and apply security protection themselves. A trusted infrastructure includes OSs and hardware platforms that offer reliability, manageability, and integration of security.

Operating Systems

When the necessary security mechanisms are built into the base of an OS, organizations can rely on standard enforcement mechanisms in the security architecture. Built-in mechanisms are harder to subvert. They also reduce dependence on correct implementation of the necessary security components in an application by (potentially) non-expert developers.

Security-relevant OS services include authentication, cryptographic libraries, intrusion detection, intrusion prevention, and compartmentalization technologies. When built into the core of the system, these security mechanisms are easier to control by policy, easier to manage across different OSs, and more reliably implemented by experts.

Hardware Platforms

The utility computing platforms of the future provide virtualization of computing resources, such as CPUs, storage devices, and networks. These platforms require integrated security mechanisms. For virtualization-derived utility computing to succeed—from VMware to HP-UX, Microsoft® Virtual Server, and Xen (an open-source virtual machine project)—businesses must be confident in the reliable separation and isolation of processes.

Modern platform and processor architectures, such as the IA-64 platform (Intel® Itanium®), are designed with security in mind. Other computing platforms in broad use today predate many of these security considerations. Most were initially designed with very different use models and functional requirements compared to today’s expectations in typical IT deployments. For example, the original IBM PC, which is largely preserved in current PCs and mass-market servers, was not designed to meet the security requirements of present-day deployments.

Self-Test for a Trusted Infrastructure

1. Can I reliably identify a device that belongs to my organization’s IT infrastructure (from one that does not)?
2. Can I tell that the firmware, software, and configuration of the devices inside my organization’s IT infrastructure are in accordance with our IT security policies?
3. Can I trust the behavior of the platforms in my organization’s IT infrastructure per our business objectives?
**HP's Strategic Focus**

HP believes that security for trusted infrastructures must be built-in and not bolted-on as an afterthought. This belief requires a new level of maturity for IT security. Generally, IT solutions must provide improved mechanisms to underpin an organization’s IT security policies, even in the face of developments such as utility computing, virtualization, and mobility.

**Achieving Security Through Open Standards**

Creating trusted infrastructures using open and industry-standard technologies is central to meeting the real needs of IT managers. Open standards make it possible to provide security that is built-in, manageable, and interoperable. The goal of enabling effective management of trusted infrastructures across large heterogeneous enterprises requires strong interoperability between vendor technologies, which requires collaboration and the development of (and adherence to) industry-wide specifications. For this reason, HP leads and participates in many standards bodies for infrastructure technologies. In fact, HP is an early founder and promoter of the Trusted Computing Group (TCG), created specifically to advance state-of-the-art technology in trusted infrastructures.

Interoperability is crucial for retaining business agility, particularly when businesses strive to achieve end-to-end security in a trusted infrastructure. HP’s efforts within organizations such as the Internet Engineering Task Force (IETF) are aimed at creating the necessary interoperability interfaces. Furthermore, efforts to advance the state of security mechanisms in the network must be combined with efforts to evolve device security. Trusted infrastructure solutions will rely on this. For example, proprietary approaches are emerging for network access-control security that will serve business needs only if they can be deployed in a truly adaptive and heterogeneous environment. They must interoperate smoothly and support the relevant industry standard(s).

HP is a leader in the standards efforts of the Trusted Network Connect (TNC) working group. The TNC is a new effort in the TCG to define an open-solution architecture that enables network administrators to enforce security policies for endpoint host connections to multi-vendor networks.

---

**Trends Topic**

**Software Integrity**

The authorization to access or modify data is usually associated with applications. However, an attacker can coerce an application into performing additional operations, thus compromising security. Malicious software can gain the privilege to modify a stored copy of an application or modify an application at runtime. It can be incorporated in an application by the user’s unwitting actions, for example, downloading executable content in the form of ActiveX controls. The modification may also be performed by some code attached to low-level software on the platform. For example, device drivers typically have read and write access to memory or at least to critical OS data structures. Other attacks may be aimed at the OS’s security mechanisms.

It is possible to detect, prevent, and respond to attacks on the integrity of software, but it requires effort. The privilege to modify software at rest (programs on the platform’s hard drive) can be restricted to a separate software installation role, which is distinct from the role of running a given application. Some critical systems apply protections through underlying hardware mechanisms, such as keeping relevant software on media (for example, a CD-ROM or flash memory) that cannot be altered at runtime. The Trusted Computing Group (TCG) specification provides mechanisms for software integrity to be measured, recorded, and tested from the start of a platform’s boot cycle. Effective use of this capability, however, requires close support from the OS.
Trusted Computing for Trusted Infrastructures

The TCG focuses on designing and standardizing security building blocks for the architecture of most types of computing platforms currently in use. This work supports the ability of those platforms to meet the growing need for more trusted infrastructure technologies. The Trusted Computing initiative collectively addresses new security requirements for computing platforms. At the same time, it preserves the openness and backward compatibility of platforms to remediate mainstream security holes and threats.

Trusted Computing Products

Trusted Computing brings aspects of high-grade security technology to commercial IT systems at a low cost. It raises the bar for available off-the-shelf technology. This is not only attractive to commercial organizations that depend on off-the-shelf technology for their IT infrastructure, but it also appeals to governments because it will allow them to use reliable and inexpensive Commercial Off-The-Shelf (COTS) technology for a broader set of applications. More generally, Trusted Computing significantly improves enterprise IT security by providing the foundation for enforceable security policies and strengthened identity mechanisms across a range of different devices.

HP has been a leader of the Trusted Computing initiative from the outset. HP’s PC business and HP Labs teams include inventors and experts in Trusted Computing who spearheaded the Trusted Computing initiative more than five years ago. Trusted Computing is a great example of bringing “HP Invent” from HP Labs and forward-looking businesses into HP product lines and out to end users.

Trusted Computing delivers some significant benefits today, and some of these are manifested in HP products such as HP ProtectTools Embedded Security. However, increased Trusted Computing benefits will be delivered when new hardware platform architectures are combined with redesigned OS software that can fully exploit the improved security attributes of the platform.


Trusted Computing Platform Functionality

The purpose of the TCG architecture is to prevent the subversion of key security features by software attacks on the platform. So that both local and remote users can trust reported information about the platform, it is necessary to protect the reporting mechanisms against software attack. The reason is obvious: the platform cannot reliably detect a software attack if its own software can be subverted. Protection against hardware attack is also necessary so that a remote user can trust reported information about a platform. This helps the remote user know, for example, that a local user has not physically tampered with the platform.

TCG History

TCPA stands for the Trusted Computing Platform Alliance. The TCPA was founded in 1999 by HP, Compaq, Intel Corporation, Microsoft Corporation, and IBM Corporation to address the issues of Trusted Computing Platforms. It is the predecessor organization of the Trusted Computing Group (TCG), which was established in 2003. The TCG was formed with a broader set of promoter members, a collection of typical industry consortium bylaws, and intellectual property agreements centered on reciprocal Reasonable and Non-Discriminatory (RAND) licensing. TCPA specifications in progress were brought into the TCG. The TCG extends Trusted Computing work to a broad set of platform technologies as well as infrastructure protocols and software stack interoperability.

Today, the premier book that discusses and explains trusted computing concepts and technology is HP’s Trusted Computing: TCPA Technology in Context. It explains the Trusted Computing vision and details its operational design, deployment, and extensibility through future development.
The Trusted Platform Module (TPM) is at the base of the trusted platform architecture. TPM is an enabling technology consisting of a dedicated security hardware device (with associated software) that meets TCG specifications. The TPM chip can be integrated with computer motherboards and many types of devices, including PDAs, laptops, cellular phones, and servers. It provides multiple security functions including:

- Device authentication
- Attestation of software state on the platform
- Protection of secrets and stored data on the platform

Figure 4–3
Example of TPM Internal Architecture

The TPM includes all the functions that must be trusted in order for the TCG architecture to provide a set of features that cannot be subverted. Figure 4–3 illustrates the internal architecture of a TPM. From a business perspective, TPM-enabled devices create a way to manage business risk, manage assets, and protect critical infrastructures. For example, a TPM can support:

- Data protection
  - Stronger encryption
  - Ease of use
- Network protection
  - Device authentication
  - Protection of network credentials
- Identity protection
  - Strong, auditable, and attestable device identities rooted in hardware
  - Built-in second factor authentication methods for protecting a user identity
- IT services and infrastructure for managing platforms
  - OS-independent hardware-based policy enforcement on the use of and access to keys and data protected by the TPM
  - Security policy compliance
  - Software and hardware configuration management
Device Authentication

Trusted platforms provide mechanisms to help establish confidence in the behavior of a platform in an IT infrastructure. The basis for this confidence rests with the declarations from recognized and trusted third parties. These third parties can endorse a platform because they have assessed and measured the integrity of the platform. If the measurements meet a specific criteria, the third party states that the platform is trustworthy for certain purposes.

To associate trust with a specific platform, the trusted third party can certify a TPM cryptographic key. Two major classes of TPM cryptographic keys can reliably identify a trusted platform: non-migratable keys and migratable keys. Non-migratable keys are locked to the trusted platform from which they originate. By contrast, migratable keys can be moved from the originating trusted platform to another system, but only under the tight control of the owner of that system (the system user or possibly an IT administrator for that system).

Migratable and non-migratable keys exist so that a TPM can use them as cryptographic identifiers to prove that it deserves a third party’s trust. For example, remote access software could use a TPM cryptographic key to uniquely identify the system in an IP security (IPsec) or an 802.1X authentication protocol to the backend of the IT infrastructure.

The concept of platform identity creates a reliable new security feature for the IT security tool kit: device authentication. Strong association of cryptographic credentials to a computing platform allows companies to personalize systems and issue credentials for recognition by the corporate network. Platform identity can also be used to configure the security credentials of a computing platform independent from OS security. This provides protection from mistakes or deliberate violation of certain security policies by OS administrators. For example, a security credential protected by TPM hardware can be controlled by specialized IT personnel (or a TPM administrator) to prevent copying or moving between machines by OS or domain administrators.

Features for device authentication are available today in a range of systems across the industry that have onboard TPMs. HP ProtectTools Embedded Security products provide features and mechanisms that can be used off the shelf for stronger hardware protection of user identity credentials, and they provide the building blocks to integrate more advanced physical device authentication to access control processes in IT infrastructure services.

Attestation of Software State

A computer platform has integrity if the OS and underlying firmware are tamper-free and applications running on the platform execute without interference. Existing security solutions assume the integrity of the platforms on which they operate. In particular, they assume that secrets can be safely stored and used on even the most open computing platforms, such as PCs.

Because platform owners are in control of their platforms’ software environment and history (including interactions, physical modification, and software execution), owners may place trust in the integrity of their platforms. However, platforms are increasingly connected and exposed to threats from the Internet, which makes this confidence questionable. A third party is in an entirely different position than the owner, because the third party usually knows nothing about the environment and history of a remote platform. A third party, therefore, has no explicit confidence in the integrity of a remote platform.

For this purpose, the TCG defines an architecture that allows a computing platform to verifiably and reliably prove its integrity. This is achieved via a TPM-based mechanism that enables reporting of software and configuration measurements to a remote party. These integrity-reporting features are known as an attestation of the software state and configuration of a system. The features are not available today.
in mainstream platforms, because they are not integrated with mainstream OSs. Starting in 2006, however, Linux systems, UNIX® systems, and the next version of the Microsoft® Windows® OS are expected to support attestation features.

Attestation mechanisms provide the anchor for new architectures that will strongly rely on state information provided by remote systems. For example, a remote access solution could require systems that request network access to first attest that they have implemented the latest enterprise-approved security measures, such as anti-virus software and desktop firewall configuration on the client device. Another example is an information-flow security solution that controls access to and manipulation of enterprise data in an enforceable manner, based on security policy.

**Protection of Secrets and Stored Data**

On a trusted platform, a TPM provides logical and physical protection of secrets and logical protection of the data protected by those secrets. The TPM acts as a conventional cryptographic coprocessor, and its integrity-reporting mechanisms can prevent the release of secrets to inappropriate processing environments.

Specifically, a trusted platform provides hardware protection for keys and other secrets that would typically encrypt files or authorize access to servers or other networks. The TPM can prevent the release of secrets conditioned upon presentation of a valid authorization value, the presence of a particular TPM, and/or the verification of a particular software state in the platform. This mechanism is known as the ability to seal storage to a given platform and/or a given software state on that platform. The TPM can therefore prevent inappropriate access to encrypted files and network resources that would otherwise be vulnerable to attacks, such as searching the contents of a hard disk, moving a hard disk to another platform, or loading software to snoop on other processes. Because the TPM can enforce such policies, it is essentially a hardware-based policy enforcement mechanism for data decryption and cryptographic credentials.

Attestation of software state and sealed storage mechanisms will only be available to applications when OSs start integrating the attestation features of the TCG architecture. As discussed earlier, this should occur in 2006. Today, HP ProtectTools Embedded Security products take advantage of the standard protected storage feature of a TPM to strengthen encryption solutions and provide a stronger tie between security credentials and a physical device.

**Elements of a More Secure Platform**

**Embedded Security and TPM**

In a PC, a TPM is attached to the low-pin-count (LPC) bus on the motherboard. A TPM provides mechanisms for root security functions and a hardware root of trust in support of OS security. Beyond providing well-understood cryptographic functions, TPM features support the design of new OS architectures that create a chain of trust, which is built from the TPM hardware root of trust and extends to software on the platform. With a TPM, a typical chain of trust can provide strong cryptographic attestation (across a network) of the state of a local platform’s firmware, hardware configuration, OS, and software configuration. Combining a TPM with higher-level software creates the basis for strong, hardware-based policy enforcement for the first time in mass-market systems. HP workstations, desktop PCs, and notebooks are available with a TPM.

**Operating Systems**

OS support is expected to gate the most widespread commercial availability of the Trusted Computing platforms. Those platforms will integrate TPM features and combine other components—such as new CPU and chipset security architectures from AMD or Intel (for example, Intel’s LaGrande Technology)—to provide security mechanisms that directly benefit higher-level applications.
As noted previously, Microsoft is expected to build on these technology components in future versions of the Windows OS and provide remote software state attestation features enabled by the Trusted Computing architecture. Linux and UNIX vendors are expected to make use of these technologies in the same timeframe to create similar capabilities for these platforms.

Applications

Today, HP’s ProtectTools products enable legacy applications to take advantage of the TPM transparently through standard interfaces such as the Microsoft Cryptographic API (MSCAPI) and the Public-Key Cryptography Standards (PKCS) #11 interface. They also provide applications designed to use a TPM to enhance data security. Newly developed applications will use TPMs on computing platforms. OSs that build a chain of trust from the TPM will also provide benefits for the management of trusted infrastructures, independent of individual applications.

Trusted Computing Across the Infrastructure

The benefits of Trusted Computing are available to virtually any device that contains a processor and an OS/environment, runs applications, and communicates with other devices via networks. The value of this emerging technology becomes greater in more open platforms; it helps attest to appropriate state and configuration without restricting and locking the platform completely. The expectation is that Trusted Computing will appear in all relevant form factors over time, including PDAs, servers, and mobile phones.

Today, the TCG has active working groups to address the different types of platforms. The working groups are designing specifications for the Trusted Computing architectures of the various device categories and their use models. All of the TCG’s work focuses on manufacturer- and vendor-independent specifications to enable interoperability of implementations.

In addition, the TCG is focusing on infrastructure protocols and mechanisms to design interoperability and support for new trusted computing features. HP leads and participates in these efforts, including the TNC working group. This work will allow the next generation of infrastructure services to seamlessly use Trusted Computing technology across multi-vendor platforms, OSs, and applications, supporting the design and deployment of truly heterogeneous trusted infrastructures.

Security and Privacy Issues

Not surprisingly, many security-enhancing technologies have privacy implications. Privacy requirements are dependent upon the context in which they are viewed. In some transaction usage models, increasing the security of data requires identification from an actor (user or system) that wants to access the data. In other models, anonymity helps ensure the security of the actor’s identity or Personally Identifiable Information (PII).

In the past, Trusted Computing was mischaracterized as a privacy threat. In fact, Trusted Computing specifications have been developed with specific, privacy-sensitive principles to allow for secure IT solutions that respect privacy. Trusted Computing contains building blocks that, used correctly, can protect the privacy of data or the actors wanting data access. Notably, the Trusted Computing specifications have consistently built privacy considerations into the design of the technical architecture. Various mechanisms support the protection of private data and avoid approaches that create privacy concerns (such as a visible, single, and unique identifier for a platform). From mechanisms that support the creation of pseudonymous identifiers to designs that let platform owners opt-in to use the technology, the technical specifications carefully consider the protection of PII.
Trusted Computing can be effectively deployed across a variety of use models with differing privacy attributes. This includes meeting the strictest privacy legislation and providing the basis of privacy-enhancing technologies for future IT solutions and platforms. HP’s ProtectTools Embedded Security products comply with the privacy-sensitive and user-control spirit of the TCG specifications. In addition, HP Labs is actively pursuing the design of new privacy-enhancing applications of Trusted Computing with the broader research community.

Secure Development

The root cause of most security incidents (beyond the perpetrator of an attack) is typically a security vulnerability. Of course, people and processes can create significant vulnerabilities, and there are many ways to track known vulnerabilities, patch them, and block them. However, this reactive approach is not sufficient. Developers must be more proactive and create less vulnerable products and solutions. This is the motivation behind HP’s secure development initiatives. For HP, secure development is an ongoing process that begins with awareness and education and continues all the way through the product life cycle. This is how HP works to produce secure and trusted products and solutions and builds in security right from the start.

Minimizing Flaws

As evidence of the importance of secure development practices, various worms such as Code Red, Nimda, Blaster, Slammer, and Sasser have caused havoc on public networks, private networks, and home systems. The root cause of the vulnerabilities they exploited comes down to a single untrusted library call, a failure to prevent a memory structure from overflowing, or some other insecure software-development practice. HP’s secure development initiatives are aimed at minimizing known bugs and flaws that have security implications. In addition, they add security technology to design and solution architectures. By incorporating secure development practices into the product design life cycle, HP can increase solution quality without impacting the product’s time to market. At the same time, HP saves support costs and end users save time and money by avoiding security issues during deployment.

Developer Education

Today, HP has a worldwide security education program targeted at all internal developers. Both general developers and security-focused developers need to learn how to make less vulnerable products. Security-focused developers also need to learn how to incorporate specific built-in security technologies. The program includes best-practice whitepapers, on-demand seminars, computer-based training modules, and instructor-led courses.

Product Development Life Cycle

Other parts of HP’s secure development initiatives focus on constantly improving product development life cycles. HP has added security-focused steps to each stage of the product life cycle. For example, risk assessment and vulnerability assessment techniques are used during the design phases, and the testing phases present the opportunity to perform both component- and system-level security testing. Processes and methodologies are brought into HP development life cycles, along with source code, application- and system-level vulnerability scanners, and threat assessment tools. HP uses both its own HP–invented tools and best-in-class tools from third-party vendors.

This effort results in products, solutions, and services that are designed with security in mind. It delivers solutions and services that not only perform specific security functions but also exhibit fewer vulnerabilities in the first place. In addition, HP Services is making secure development practices and expertise available directly to customers. Secure development services from HP include education and training as well as threat and vulnerability assessment.
Network Security

The enterprise network connects all other trusted infrastructure elements. A properly secured network protects and integrates its hosts, while remaining functional in the face of business-driven change and today’s countless threats to information availability, integrity, and confidentiality. This section focuses on data network security and limits its coverage to IP-based networks. It discusses network security threats, defenses, design, and the selection of specific network security components.

Environment

Enterprise networks are changing. Modern networks have a diversity of components with varying trust levels; they are no longer simply fortresses encircled by defensive rings. Traditional enterprise networks have an internal compartment devoted to internal communications and a carefully isolated compartment—commonly called a demilitarized zone (DMZ)—devoted exclusively to externally accessible services. Firewalls control access between the internal network and the DMZ, and between the entire network and the Internet.

Three factors have caused the enterprise network to change dramatically: Internet delivery of services, telecommuters and mobile workers, and outsourcing. These factors are illustrated in Figure 4–4.

Internet Delivery of Services

Organizations use the Internet to deliver increasingly complex services in intra- and inter-domains, including collaboration and transactions with vendors, customers, and partners. This process often relies on interactions between groups of systems on different enterprise networks. Therefore, external services hosted in the DMZ interact with internal systems in increasingly complex ways, complicating the relationship between the DMZ and the internal network.
Telecommuters and Mobile Workers

Organizations rely on telecommuters and mobile workers to perform critical tasks that require access to internal applications and data. Organizations must provide access to internal resources from almost any location and for a variety of devices over which they have varying degrees of control. These requirements further blur the network perimeter.

Outsourcing

Organizations are distinguishing between their core competencies and other business-critical activities in order to better compete in the global economy. Many organizations are aggressively outsourcing critical work to distant partners or delivering global services based on their core competencies. IT has responded by making internal applications available externally via virtual private networks (VPNs), leased connections, terminal serving, and reverse proxies.

Taken together, these three trends result in networks with a variety of users, segments, and hosts that are authorized to do different things and are trusted at different levels. Fortunately, while networks have become more complex, their security capabilities have become more sophisticated and autonomous.

Network Security Analysis and Planning

Network security addresses enterprise network technologies that connect to the Internet and to extranets in addition to the boundary of the IT infrastructure. Network security must also focus on the security of wireless networks. Controlling access to network resources and providing lower-level prevention and detection of attacks allows enterprises to optimally protect their information assets.

Approach

A traditional approach to network security implementations is to encircle an unsecured network with a perimeter defense solution that controls access to the network. Perimeter defense is an integral part of an overall defense strategy. However, within the perimeter, a user left unrestricted may cause intentional or accidental damage. The network can be extremely vulnerable to a hostile party gaining access to a system or application inside the perimeter, and it can be compromised by an authorized user.

Deploying a collection of security techniques and tools, including firewalls, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), and VPNs, can help enterprises to ensure overall network security.

Understanding Security Risks

Evolving regulatory and legal requirements are increasing enterprise risk exposure to a level where IT risk management should be a top priority. Network administrators face a witch's brew of dangers: vulnerability scanning; denial of service (DoS) attacks; hijacking of networks to do harm elsewhere; defacement of public web sites; physical intrusion into sensitive areas; abuse of kiosks, hotspots, and other public computing facilities; wide distribution of high-quality attack tools; network mapping and port scanning; vulnerability scanning; war dialing; and war driving. The list seems endless.

As stated previously, the dangers do not always come from the outside. External threats can also be realized by internal attackers who may be employees or contractors engaged by the enterprise. Another area of vulnerability is a trusted network connection, such as a connection with a vendor or trading partner, that has experienced a network security breach.

Understanding and Mitigating Network Security Threats

This section discusses types of security threats, attack categories, and specific attack and mitigation methods.
Security Threat Categories

There are four general categories of security threats to the network:

1. **Unstructured threats** consist of random attackers using a variety of tools to attempt to crack protected systems. The tools used include password crackers, credit card number generators, and malicious shell scripts, among others.

2. **Structured threats** are usually generated by technically competent individuals or organizations. They seek to obtain access to highly sensitive data, and their attacks include development of sophisticated attack plans. They are often sponsored by organized crime, industry competitors, or state-sponsored intelligence organizations.

3. **External threats** include structured and unstructured attacks. They may be random errors or attacks with malicious or destructive intent.

4. **Internal threats** usually involve disgruntled or former employees. These threats seem the most ominous, but measures are available to mitigate them. Internal threats may be a result of user ignorance, a knowing violation of security policies, access of malicious web sites, or a download or received e-mail that contains viruses, worms, spyware, or other malware.

Attack Categories

Attacks that compromise resources consist of four basic categories:

1. **Reconnaissance attacks** occur when an attacker attempts to discover and map systems, services, and vulnerabilities.

2. **Access attacks** occur when an attacker attempts to retrieve data, gain access, or escalate access privileges.

3. **DoS attacks** occur when an attacker attempts to disrupt the service that a resource normally provides.

4. **Worm, virus, and Trojan horse attacks** occur when an attacker attempts to damage or corrupt a system, replicate malicious code, or deny services or access to network resources.

Mitigating Reconnaissance Attacks

Reconnaissance attacks are performed with packet sniffers, port scans, ping sweeps, Internet information queries, or vulnerability scanning software.

*Packet Sniffers*

A packet sniffer captures data that is transmitted in cleartext on the network. Examples include user names and passwords transmitted in applications such as telnet, FTP, and e-mail. Detecting the sniffer is difficult unless direct access is available to the system running the sniffer.

Mitigation strategies for packet sniffers include:

- **Secure password mechanisms** are the first mitigation effort to thwart packet sniffers from capturing user names and passwords. The options in this area include one-time passwords or encrypting the authentication handshake between a client and a server. Because they are typically good for a short time period, such as a minute, even one-time passwords should not be transmitted in the clear whenever possible.

- **Anti-sniffer tools** detect the presence of a sniffer on the network. They must be in place for a period of time in order to detect anomalies that occur when an unauthorized sniffer is launched on the network.

- **Switched network infrastructures** greatly reduce the effectiveness of packet sniffers in the enterprise.

- **Cryptographically secure channels** for transmitting data are the best way to render a packet sniffer irrelevant.
Port Scans and Ping Sweeps
Port scans and ping sweeps cannot be prevented entirely. IDS systems at the network boundary and on
the host can detect these types of attacks and notify the administrator that an attack is underway.

Internet Information Queries
Domain Name System (DNS) queries can reveal the IP addresses of systems on a network. This can
be very useful for IT personnel to manage the network. On the other hand, an attacker can use the IP
addresses to launch a ping sweep to map the network, and then a port scanner can be used to provide
a list of all services running on the network.

Vulnerability Scanning Software
These tools are typically intended to enable IT personnel to efficiently find vulnerabilities such as
permissively configured hosts, missing patches, and weak passwords. In the hands of an attacker, how-
ever, they can point to a successful attack.

IDSs can detect patterns of activity associated with vulnerability scanning. In addition, internal use
can be controlled by clear and well-enforced policies: only security personnel should be authorized to
use vulnerability scanning software. Of course, properly patched and configured systems also play a
key role.

Mitigating Access Attacks
Access attacks can take the form of password attacks and trust exploitation attacks.

Password Attacks
Password attacks are executed by malicious users in order to retrieve data or escalate privileges. They
are mitigated as follows:

- **Use strong passwords.** Characteristics of strong passwords include at least eight characters, upper-
and lower-case characters, numbers, and special characters. Password management software can
require strong passwords. A key element is training users and enforcing password policies, for
example, forbidding employees to keep passwords on sticky notes at their desks.

- **Expire passwords regularly.** Password expiration periods depend on the business risks associated
with unauthorized access to the protected data or systems, the likelihood of password compromise,
and the expected frequency of password use.

- **Disable accounts.** After a specific number of unsuccessful password attempts, the user account
should be disabled.

- **Do not transmit plaintext, static passwords.** Use one-time passwords or encrypted authentication
credentials.

Trust Exploitation Attacks
Trust exploitation attacks involve a user or system taking advantage of privileges that a system has grant-
ed (either to all users or to specific users) without an appropriate level of authentication. Systems on the
outside of a firewall should never be entirely trusted on the inside of the network. All too often, systems
or network administrators establish trust between a user and some data based solely on an IP address.
For example, a network administrator might allow access to an internal web site from the Internet
based on an IP address at a user’s house. This is an insecure access method because an attacker could
use (spoof) the same IP address.
Examples of trust exploitation attacks include *man-in-the-middle* and *port redirection*. In a man-in-the-middle attack, the attacker becomes an intermediary in a communication session between two nodes in order to capture or alter information. Port redirection works by compromising a target system to listen on a certain configured port and redirect all packets to a secondary destination.

Trust exploitation is mitigated by preventing trust between external hosts and internal hosts, properly authenticating users, and using secure protocols for sensitive communication sessions.

**Mitigating Denial-of-Service (DoS) Attacks**

DoS attacks are defined simply by their name: the attacker denies a particular service that is normally available to users. It is important to note the method that an attacker uses to execute a DoS attack. The most common type of DoS attack is a Distributed DoS (DDoS). This type of attack is executed through the distribution of malicious code to a large number of systems. The most common delivery methods are distributing e-mail attachments and exploiting target systems in order to deposit the DDoS code.

DoS and DDoS attack mitigation is straightforward, but it is difficult to completely eliminate vulnerability to DDoS attacks. Mitigation includes proper anti-spoofing configuration of routers and firewalls and the use of anti-DoS features on routers, firewalls, and hosts.

**Mitigating Worm, Virus, and Trojan Horse Attacks**

A worm executes arbitrary and often malicious code on a host, copies itself to the system’s memory, and then copies itself to other computers. A virus is a piece of software attached to another program. When the user’s normal program launches, the virus executes and causes unwanted or malicious actions on the host computer. A Trojan horse is different in that it is written to appear entirely benign. However, it executes malicious activities on the host computer.

Mitigation of worm, virus, and Trojan horse attacks is fairly straightforward, but in a large enterprise it can be a challenging task. Mitigation is accomplished through properly using anti-virus software and updating anti-virus signatures. Effective use of anti-virus software also includes installing it on enterprise servers—especially mail servers because e-mail is a significant delivery method for these attacks.

**Principles of Design**

Network security is an exacting discipline, and successful implementation requires much attention to detail. Measures that harden and secure the network against internal and external attacks include:

- **Segregating older systems** within their own network segments and using access control rules, firewalls, and other techniques to protect them
- **Deploying firewalls** at the network level (via network hardware devices, servers, or other products) and on individual workstations and devices
- **Hardening the TCP/IP stack** with restrictive settings
- **Deploying port and packet filtering** features built into operating systems (OSs)

As with any complex endeavor, however, the right overall direction is essential. A few vitally important principles stand out for any network type and use. These principles should be used to orient the design effort—along with good security policies, mitigation strategies, techniques, and tools. Table 4–1 presents an overview of key design principles. More detail about each design principle can be found in Appendix A.
Table 4–1
Key Principles of Design for Network Security

<table>
<thead>
<tr>
<th>Type</th>
<th>Key Points</th>
<th>Benefits</th>
<th>Cautions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standardization</td>
<td>Reduces complexity</td>
<td>Reduces the number of threats, risks, and vulnerabilities to identify</td>
<td>Does not prevent a single successful attack from being replicated widely</td>
</tr>
<tr>
<td></td>
<td>Deploys widely tested and trusted tools throughout the enterprise</td>
<td>Reduces the number of countermeasures to implement</td>
<td>Requires some diversity for a layered, resilient defense</td>
</tr>
<tr>
<td></td>
<td>Benefits from balancing with diverse architectures</td>
<td>Uses widely tested and trusted approaches</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Conserves resources</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Least Privilege Access</td>
<td>Requires robust means of establishing and managing digital identities</td>
<td>Prevents unnecessary resource access</td>
<td>Requires sophisticated tools and processes for user privilege administration</td>
</tr>
<tr>
<td></td>
<td>Grants minimum access to systems or networks needed for business requirements</td>
<td>Mitigates the associated risks of resource misuse</td>
<td>Requires a greater financial investment</td>
</tr>
<tr>
<td>Layered Defense</td>
<td>Spans physical, technical, and administrative security measures</td>
<td>Protects the enterprise with multiple forms of defense</td>
<td>Makes networks more complex and expensive</td>
</tr>
<tr>
<td></td>
<td>Limits risk by combining countermeasures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redundancy</td>
<td>Requires justification by business needs</td>
<td>Enables networks to withstand failure of individual components</td>
<td>Makes networks more complex and expensive</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enables networks to withstand successful attacks on individual components</td>
<td></td>
</tr>
<tr>
<td>Compartmentalization</td>
<td>Uses logical, not physical, compartments</td>
<td>Defines access policies centrally and implements them at compartmental boundaries</td>
<td>Requires careful design</td>
</tr>
<tr>
<td></td>
<td>Works with geographically dispersed systems</td>
<td>Accepts changes in business structure and operations without requiring changes to the physical network</td>
<td>Requires increased cost and complexity with increasing number of compartments</td>
</tr>
<tr>
<td></td>
<td>Facilitates layered defense and standardization; flexible and adaptable</td>
<td>Contains security breaches to mitigate damage to the overall network</td>
<td></td>
</tr>
</tbody>
</table>

Securing Network Perimeters and Extranets

The first security measure in most enterprises is a perimeter defense. Enterprises have become very dependent on firewalls and other perimeter protection systems to safeguard their networks. Because it is difficult to secure all the systems in an enterprise and keep them secure, it is necessary to rely on the perimeter as the first line of defense.

Traditionally, firewalls have been mistakenly viewed as magic black boxes; enterprises have a propensity to install them and forget about them. Perimeter security planning and design should begin with risk assessment and consider perimeter defense strategies and standards such as defense-in-depth (layered defenses), trust zones, and hardened systems. Perimeter security implementation should encompass routers, dial-up modems, switches, wireless networking, firewalls, IDSs/IPSs, VPNs, and ongoing network security assessments.

Virtual Private Networks (VPNs)

VPNs enable organizations to use the public Internet for secure communications. VPNs provide authentication, confidentiality, and message integrity services that enable organizations to trust information sent over the Internet. The VPN Consortium (VPNC; www.vpnc.org), an international trade organization for manufacturers in the VPN market, specifies three VPN technologies:

- **IPsec with encryption in either tunnel or transport modes**
- **IPsec over Layer 2 Tunneling Protocol (L2TP)**
- **Secure Sockets Layer (SSL) 3.0 or Transport Layer Security (TLS) with encryption**
According to the VPNC, all traffic on a secure VPN must be encrypted and authenticated, the security properties of the VPN must be agreed to by all VPN participants, and no one outside the VPN can affect the security properties of the VPN. In addition, an administrator who knows the extent of the VPN must control secure VPNs. Appendix B details how the VPN technologies specified by the VPNC enable secure communications.

Securing Wireless Access

In many ways, wireless security is just like wired security; the issues are largely the same. Regardless of the medium, every system needs to safeguard proper authentication, privacy of transmission, prevention of viruses, and protection against DoS attacks. The differences arise from the fact that mobile devices and their transmissions over an unshielded medium (air) are inherently more vulnerable to impersonation, sabotage, and interception.

Device Security

Mobility has extended the device spectrum from traditional desktops and servers to laptops, handhelds, phones, and a wide range of specialized appliances. These devices are vulnerable to a new set of security issues, including susceptibility to loss and theft, increased use outside company premises, and less processing power to ward off threats.

Generally, device security falls into three areas:

- Securing local data from unauthorized access
- Safeguarding the device from malicious threats or data loss
- Protecting connectivity between the device and the applications residing on corporate servers

Securing Local Data from Unauthorized Access

The most common concern relating to mobile device security is that sensitive information stored locally may be prone to unauthorized access. One fundamental distinction of mobile devices is that they can be used off-site in public (even adversarial) environments. A secure solution needs to start with physical security, for example, cable locks. It should extend to restricted access control (strongly authenticated logon) and possible storage encryption.

Safeguarding the Device

Like other systems, safeguarding applications and data is a concern for mobile devices. Virtually all systems have information that is important to users, and reconstructing the configuration of the applications and platform is never a pleasant task. In addition, there is also the need to cope with a lost device or a virus infection and get the user back to work as quickly as possible. Therefore, safeguarding devices calls for a multifaceted approach involving some combination of asset control policies and procedures (for example, what to do if a PDA is lost), physical security, device backup or synchronization, mobile platform standardization, strong authentication, and storage encryption. Of course, the first step in risk management is always to understand the organization’s specific risk environment.

Fortunately, the reduced computing power and functionality of mobile devices have thus far made them less of a target to virus attacks than their desktop counterparts. However, this immunity is not expected to continue. The HP iPAQ Pocket PC is easily powerful enough to inflict a virus on itself and others, and concept viruses have started to appear on both phones and PDAs. (For information about ProtectTools Windows Mobile, which enhances security for the Microsoft Windows Mobile platform, see the HP Host Security Products and Solutions section of this chapter.)
Protecting Connectivity

In most cases, mobile users want to connect to their enterprise networks and access applications. These connections and actions need to be protected beyond the scope of the device. Users need to be able to establish a secure connection over a typically wireless transmission medium. In some cases, the device can connect directly to the private network, but oftentimes its path traverses some type of public network.

Popular public packet data networks include Wireless LANs (WLANs), General Packet Radio Service (GPRS), Cellular Digital Packet Data (CDPD), or even circuit-switched connections dialed up to an ISP. If IP networking is supported, the user may establish an IPsec or SSL VPN connection to the corporate infrastructure. For detailed information about wireless security technologies including Wireless Personal Area Networks (WPANs), WLANs, and Wireless Wide Area Networks (WWANs), refer to Appendix C.

Enterprise Requirements

Enterprises typically have a multi-level security structure. The first level is the perimeter of the corporate network. To reduce the threat of industrial espionage or deliberate sabotage, only employees, authorized contractors, or other business partners (via an extranet) are allowed access. Although this safety net is difficult to enforce entirely, it does thwart the attempts of casual attackers and creates an obstacle for sophisticated intruders. What does this mean for wireless implementations? First, the secured perimeter must be accessible to mobile devices. Second, information used to access the perimeter from mobile devices must be encrypted to ensure that it is not intercepted or falsified. Typically, the solution to both of these problems is a VPN.

The most sensitive applications need to maintain an additional level of security configuration that includes authentication, authorization, and auditing (AAA). Users who have a business need to access the application must authenticate to the application first. Depending on their roles and responsibilities, users may be given different authorization levels (read-only, modify, delete) or authorization to subsets of the data. All the actions requested and performed are logged to preserve an audit trail.

Best Practices for Secure Networks

Management

Management best practices for secure networks include well-defined and enforced policies, standards, user training, procedures, standard locked-down baseline configurations, and guidelines. Other areas of concern are extranet user agreements and the proper handling of worker termination. Specific engagements such as security reviews, risk and vulnerability assessments, and incident and event management must also conform to industry best practices. A good reference for security management practices is the Information Security Management Handbook, by Harold F. Tipton and Micki Krause, Auerbach Publications, 5th Edition 2004, ISBN 0-8493-1997-8.

Operations Security

A trusted infrastructure depends on operational continuity and sustainability. This requires best practices for implementing a consistent approach to selecting and deploying infrastructure components and ensuring sufficient capacity to establish a robust, scalable, and highly available infrastructure. Operational sustainability also provides common supporting operations for backup, disaster recovery, replication, and business continuity.

Operations security represents the controls and safeguards that secure an enterprise's information assets on a computer or linked with the computer environment. Security controls address software, hardware, and processes. As the core component of information security, operations security controls the way data is accessed and processed, and it represents a set of controls designed to provide effective levels of security.
Operations security provides consistency across all applications and processes. It includes protection of physical assets, such as computing equipment, networks, and media. Operations security also includes resource protection, accountability access and use, and audit trails.

- **Resource protection** prevents the loss or compromise of an enterprise’s computing resources, including main storage, storage media, communications software and hardware, processing equipment, standalone computers, mobile devices (as appropriate), and printers. Resource protection helps reduce potential damage from unauthorized disclosure and alteration of data by limiting opportunities for misuse.

- **Accountability access and use** ensures access for a specific authenticated and authorized individual user or system at a particular moment in time, and it tracks access and use to that individual or system.

- **Audit trails** track activity to specific individuals or systems to determine accountability and responsibility. Operations controls for protecting resources require accountability and responsibility for all of those involved in developing, maintaining, and utilizing processing resources.

### Physical Security

Physical security consists of controlling access to physical assets such as buildings, computers, and documents. Such assets can hold sensitive information and provide access to networked resources. Enterprises implementing physical security must plan the appropriate level of security for and access to site locations, buildings, computer rooms, and data centers. Managing and monitoring these facilities is a major component of physical security. To address physical security needs, enterprises must define:

- Best practices for the management and monitoring of physical facilities
- Mechanisms for protecting removable media and offline data storage
- Methods of securely labeling and protecting confidential documents

### Firewalls

Firewalls secure network perimeters, workgroups, and hosts. They can be configured to block unauthorized incoming and outgoing traffic, conceal system identities and network topologies, log traffic, and log events of interest. Some firewalls have routing capabilities to direct incoming traffic appropriately, and some firewalls are used to authenticate network users. However, firewalls cannot defend against attacks that do not use the network or use it in an authorized fashion, for example, an internal attack or malicious code downloaded from the Internet.

Firewalls can operate on a variety of platforms, including general-purpose servers, dedicated appliances, and desktop computers. The OSs of general-purpose servers must be carefully hardened to provide a secure environment for the firewall. This hardening process generally involves setting system parameters and disabling unnecessary system services. This process is not necessary for appliance-based firewalls, which come with their own vendor-configured and supported hardware. Desktop firewalls control traffic to and from the host upon which they reside, and they are installed directly on the desktop computer.

There are several different types of firewalls, including packet filters, circuit-level gateways, stateful inspection firewalls, and application proxy servers. They use different techniques to determine whether traffic should be allowed or blocked, and they operate at different layers of the Open System Interconnection (OSI) standard reference model set forth by the International Organization for Standardization (ISO), as noted in Table 4–2 on the following page. For details about these firewall types, refer to Appendix D.
Table 4–2
Types of Firewalls and OSI Layers of Operation

<table>
<thead>
<tr>
<th>Type</th>
<th>Layer of Operation (OSI Model)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Filters</td>
<td>Network</td>
</tr>
<tr>
<td>Circuit-Level Gateways</td>
<td>Session</td>
</tr>
<tr>
<td>Stateful Inspection Firewalls</td>
<td>Network, transport, potentially others</td>
</tr>
<tr>
<td>Application Proxy Servers</td>
<td>Application</td>
</tr>
</tbody>
</table>

Authentication, Authorization, and Auditing (AAA) Servers

Triple-A (AAA) servers authenticate network users, authorize them to use particular network resources, and account for their network usage. They provide a central control point for external network access, and they work with various types of network access servers that interact with users and collect their credentials. AAA servers are mentioned here because network access is a key element of a trusted infrastructure. The Identity Management chapter of this handbook provides further details about AAA technology. See Appendix E for a summary of AAA protocols.

Quarantine

A useful and increasingly widespread adjunct to enterprise network access control measures is to inspect the state of a host before allowing it to attach to the network. The inspection checks that the host is compliant with enterprise standards, for example, standards for anti-virus software, anti-spyware software, OS patches, and personal firewalls. If the host meets the requirements of the enterprise network access policies, it is allowed to access the network. If not, it is quarantined on a private network space (out of reach of the main network) until it has been cleaned, disinfected, and verified safe for network access.

Intrusion Detection and Prevention Systems

Networks are still vulnerable to external and internal attack, even if they are properly secured and every effort is made to control host security. IDSs and IPSs provide an extra layer of defense. An IDS detects and reports exploitation of network and system vulnerabilities, whereas an IPS detects such exploits and takes immediate action to thwart them.

IDSs may be host-based or network-based. Host-based IDSs reside on servers and analyze audit logs and other indicators of system activity. Network-based IDSs use dedicated hosts that intercept and analyze network traffic. IDSs detect intrusions and other exploits such as privilege abuse by using predefined rules, predefined attack signatures, or observed deviations from normal activity (statistical anomalies).

IPSs take the idea of an IDS to the next step. After detecting an attack, an IPS performs specific actions to block an attempted attack or render it worthless. Like an IDS, IPSs may be host or network based. IPSs may respond to an attack by dropping suspicious data packets, terminating suspicious sessions, denying user access to resources, reporting activity to other hosts that may also be vulnerable, or updating their own configurations to better address specific attacks. IPSs can integrate with firewalls, so that when an IPS detects a source of hostile traffic, the firewall works to block it.
HP Network Security Products and Solutions

This section provides an overview of HP's offerings, services, and solutions related to network security. For further information, please see www.hp.com/go/security/trusted.

Adaptive Network Architecture

HP's Adaptive Network Architecture (ANA) is a blueprint for:

- Segmenting or compartmentalizing an enterprise network based on the business needs of applications or hosted services
- Extending the compartments as required regardless of location
- Providing centralized policy management for the resulting architecture

Conventional perimeter defenses can no longer balance between fast-changing business needs and sufficient protection of company information assets. Today, management of enterprise firewalls is typically exception-based, with a large number of access holes that accommodate specific user or system requirements. These exceptions cause both security and operational concerns. ANA transforms legacy enterprise data network architecture from a monolithic perimeter to a set of purpose-built (and more secure and manageable) distributed network compartments.

Compartmentalizing is not new; enterprises have been doing it for years but in a limited fashion. Traditionally, it has not been cost effective for companies to compartmentalize the entire network—conventional approaches are not scalable or sustainable. As a result, companies only compartmentalize a small portion of their network. Implemented internally within HP since 1999, ANA breaks through this barrier by combining processes, technology, and a governance model. The governance model is a tested, hierarchical arrangement where business units, IT architecture, network engineering, and network operations interact at various levels to instill agility and consistency for planning and executing change to network access policy.

There are two areas that demonstrate the capability of ANA: IP Telephony (IPT) deployments and network admission control (802.1X) adoption. In both cases, a generic access policy must be applied hundreds of times throughout the network. As business needs evolve and change, modifying such a policy on a global scale is arduous. ANA enables agility by providing a means to manage policy centrally and enforce it decentrally. With ANA, changing a hundred geographically distributed networks to permit or deny a specific application service can be handled in hours instead of days or weeks needed by conventional practices.

HP has five patents pending for the process and design elements that form the underpinnings of ANA and has successfully deployed ANA worldwide for internal operations. ANA has enabled HP to reduce network administration costs and operating expenses, while shortening lead times for acquisitions and external collaboration.

Those interested in ANA have two options. HP Services Consulting and Integration designs ANA into customer networks, and HP Managed Services delivers ANA to its outsourcing customers.

HP Active Countermeasures

The Active Countermeasures Service is a powerful tool for locating and dealing with vulnerable systems and protecting against worms and viruses in an enterprise network. Invented by HP and used internally since 2002, it is now being developed into an HP Services offering. Active Countermeasures performs regular, controlled, and targeted scanning for specific vulnerabilities. It then takes precise actions on the vulnerable systems it finds to reduce or remove the threat and notifies network managers. Details about Active Countermeasures can be found in the Proactive Security Management chapter.
HP ProCurve Networking

For nearly 20 years, HP ProCurve Networking has been building enterprise LAN products that help people run their businesses more effectively. By providing a complete and affordable portfolio of network security solutions and services, alongside HP’s highly skilled professionals, these products can help manage information resources, provide consistent performance, and deliver secure access to the enterprise.

Enforcing security at a central point gives malicious traffic an opportunity to infiltrate the network from the edge to the core. Stopping any unauthorized or suspicious activity at the edge or access point immediately isolates the problem and reduces the chance that the network as a whole will be impacted. This approach prevents users from gaining unauthorized network knowledge or performing electronic snooping to uncover passwords or other critical information that might assist in a network attack.

HP ProCurve’s unified approach addresses both wired and wireless access and secures end-user access methods to the enterprise LAN. If a security breach cannot infiltrate the host because network intelligence locks out the potential attacker, enterprise network security improves dramatically. HP ProCurve’s security-to-the-edge solutions include a framework of access security, management security, and attack resiliency as shown in Figure 4–5.

Figure 4-5
HP ProCurve Networking Framework

<table>
<thead>
<tr>
<th>Access security controls which users have access to systems and how they connect in a wired and wireless world. HP ProCurve provides:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Standard 802.1X port-based access control for all HP ProCurve enterprise-class managed products.</td>
</tr>
<tr>
<td>• A combination of 802.1X with 802.1Q standards for two levels of security. When a user authenticates via 802.1X, HP ProCurve switches can easily place the user on the appropriate VLAN based on information from the authentication server. Authorized users can be limited to exactly the network resources they are allowed to access.</td>
</tr>
<tr>
<td>• 802.1X used with 802.11 wireless networks to ensure only authorized users are granted access to the enterprise network.</td>
</tr>
<tr>
<td>• Restrictions that can be efficiently implemented at the network edge to control access rights and privileges that each user or group has to specific network resources, such as individual subnets, servers, or applications.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Management security includes the protection of the network infrastructure itself and prevents unauthorized users from overriding other security provisions. HP ProCurve provides:</th>
</tr>
</thead>
</table>
• Secure controlled access to the configuration and management of the network infrastructure
• Switches that can authenticate network managers in a number of ways
• Protection of remote management access to the console prompt using the SSH protocol

**Resiliency** relates to designing a network infrastructure to survive an attack without interrupting service. Network-based viruses can infect authenticated laptops and PCs when they connect to the Internet outside of the office. In addition to attacking network components, these viruses can compromise the network from within. With HP ProCurve:

• Products come with a number of built-in features that improve the resiliency of the network in the face of virus outbreaks.
• Management functions are protected from broadcast storms, flooded traffic, and network loops, enabling access to switch management in the presence of these network anomalies.
• Products help reduce excessive broadcast traffic that impacts every station on the network and typically results from an erroneous situation.
• Software releases run through extensive testing before distribution. One of the many standard regression test suites includes the CERT/CC vulnerability test suite that bombards a switch with network attacks.
• Routing switches support authenticated updates from authenticated routers.

**Figure 4–6**
HP ProCurve Enterprise LAN Total Security Solutions

HP ProCurve security solutions (Figure 4–6) move important access decisions and policy enforcement to the edge of the network where users and applications connect. Core resources are freed to provide the high bandwidth interconnect functions they are meant for, which means enterprise networks are optimized to perform better. What is more, effective control to the edge helps enforce security policies necessary for network convergence and a mobile workforce.

HP ProCurve Networking solutions have several layers of built-in security and take advantage of the latest standards-based security features to protect data. HP ProCurve’s diverse array of security products and services bring trust, reliability, and flexibility to enterprise networking.

**HP ProCurve Networking: HP Virus Throttle Software**

As every information-technology manager knows, computer virus epidemics are only getting worse. Current methods to stop the propagation of malicious agents rely on the use of signature recognition to prevent hosts from being infected. While this approach has been effective in protecting systems, it has
several limitations that decrease its effectiveness as the number of viruses increases. Signature recognition is fundamentally a reactive and case-by-case approach. The latency between the introduction of a new virus or worm into a network and the implementation and distribution of a signature-based patch can be significant. Within this period, a network can be crippled by the abnormally high rate of traffic generated by infected hosts.

Virus throttling, in contrast, is based on the behavior of malicious code and how it differs from unaffected code. Normally, a computer makes fairly few outgoing connections to new computers and is more likely to regularly connect to the same set of computers. This is in contrast to the fundamental behavior of a rapidly spreading worm, which attempts many outgoing connections to new computers. For example, computers normally make approximately one connection per second; the SQL Slammer virus tries to infect more than 800 computers per second.

HP Virus Throttle software establishes a rate limit on connections to new computers. Normal traffic remains unaffected, but suspect traffic that attempts to spread faster than the allowed rate is slowed. This creates large backlogs of connection requests that can be easily detected. Once the virus is slowed and detected, technicians and system administrators have time to isolate and remove the threat.

A virus-throttle approach differs from signature-and-patch approaches in three key ways:

- It focuses on the network behavior of the virus and prevents certain types of behavior, in particular, the attempted creation of a large number of outgoing connections per second.
- It restricts the code from leaving the system instead of stopping viruses from entering the system.
- It makes the system robust and tolerant to false positives by allowing connections beyond the permitted rate to be blocked for configurable periods of time.

HP Virus Throttle software should complement, not replace, signature-based solutions. The virus-throttle technology fills a gap in anti-virus protection that has, until now, allowed previously unknown threats to wreak significant damage before patches can be deployed. With HP Virus Throttle, previously unknown threats can be mitigated, giving administrators time to deploy signature updates and patches. Figure 4–7 illustrates the process employed by HP Virus Throttle software.

---

Figure 4–7

HP Virus Throttle Process
HP ProCurve Networking Secure Access

HP ProCurve Networking Secure Access appliances sit transparently in the switching fabric at the edge of the network. These network access control appliances screen users and devices to restrict access within the network, inspect traffic for pattern anomalies, and enforce all remediation policies distributed by the control server. They also work with patch management products to ensure that a device’s software revision levels and patches are current before it is admitted to the network.

HP ProLiant Essentials Intelligent Networking Pack

HP ProLiant Essentials Intelligent Networking Pack is a software solution available for HP ProLiant servers running Microsoft® Windows® 2000 and Microsoft Windows 2003. It offers advanced networking and combines capabilities for redundancy and load balancing. HP Virus Throttle software, described previously, is also implemented in this product. When implemented with other virus-prevention tools, HP ProLiant Essentials Intelligent Networking Pack provides an extra layer of protection against attacks that can bring down the entire network.

HP ProLiant DL320 Firewall/VPN/Cache Server

The HP ProLiant DL320 Firewall/VPN/Cache Server running Microsoft Internet Security and Acceleration Server 2004 provides an affordable, integrated, easy-to-use, and manageable hardware security and caching solution. It can be quickly deployed to help protect key business applications, such as Microsoft Exchange Server, Outlook Web Access, Internet Information Services, and SharePoint® Portal Server.

In addition, Microsoft Internet Security and Acceleration (ISA) Server 2004 integration with Windows Active Directory® services enables administrators to use the solution to apply group- and user-level policy and authentication across a broad range of scenarios, including firewall policy, VPN authentication, and outbound web proxy and access control.

HP IPFilter/9000 (for HP-UX 11.00 or 11i)

HP IPFilter/9000 filters IP packets that access HP-UX servers. IP packets are granted or denied access to or from the system based on stateful packet inspection and sophisticated packet-filtering rules. An HP Service Professional can remotely install and configure IPFilter/9000 on a qualified HP 9000 system and verify that the software starts up and shuts down without error.

HP Partner Secure Network Offerings

To provide a complete and integrated set of options, HP has partnered with leading vendors whose products and services enhance and complement HP products and services. Table 4–3 on the following page summarizes some of these partner offerings. See www.hp.com/go/security/strategy for details and updates about HP partner information.

Computers normally make approximately one connection per second; the SQL Slammer virus tries to infect more than 800 computers per second. HP Virus Throttle software establishes a rate limit on connections to new computers without affecting normal traffic.
### Table 4–3
Examples of HP Partner Secure Network Offerings

<table>
<thead>
<tr>
<th>Partner</th>
<th>Product Name</th>
<th>Purpose</th>
<th>Partner Web Site</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Systems</td>
<td>Cisco Clean Access</td>
<td>Enforces network security policies</td>
<td><a href="http://www.cisco.com">www.cisco.com</a></td>
</tr>
<tr>
<td></td>
<td>Cisco Secure Access Control Server (ACS) for Windows</td>
<td>Manages user access to Cisco devices and applications with 802.1X access control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco VPN-Enabled/Optimized Routers</td>
<td>Supports IPsec VPN features within Cisco routers</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cisco PIX 500 Series Firewalls</td>
<td>Provides stateful inspection, IPsec VPN, IPS, and other solutions for a wide range of device applications</td>
<td></td>
</tr>
<tr>
<td>Internet Security Systems</td>
<td>Proventia and RealSecure product lines for IDS/IPS</td>
<td>Provides IDS and IPS solutions</td>
<td><a href="http://www.iss.net">www.iss.net</a></td>
</tr>
<tr>
<td>Microsoft Corporation</td>
<td>Internet Security and Acceleration (ISA) Server</td>
<td>Provides application-layer firewall capabilities, VPN, and web caching</td>
<td><a href="http://www.microsoft.com">www.microsoft.com</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Integrated with HP ProLiant DL 320 Firewall VPN Cache server</td>
<td><a href="http://www.hp.com/go/proliant">www.hp.com/go/proliant</a></td>
</tr>
<tr>
<td>Nokia</td>
<td>Nokia Firewall/VPN appliances</td>
<td>Provides an integrated solution for secure Internet communications and access control using Check Point firewall and VPN software</td>
<td><a href="http://www.nokia.com">www.nokia.com</a></td>
</tr>
<tr>
<td>Sygate</td>
<td>Sygate Security Agent</td>
<td>Protects network-enabled endpoints through firewall and IPS engines</td>
<td><a href="http://www.sygate.com">www.sygate.com</a></td>
</tr>
<tr>
<td></td>
<td>Sygate Management Server</td>
<td>Establishes and reports on network security policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sygate Universal Enforcement</td>
<td>Ensures compliance with security policy before permitting network access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sygate On-Demand</td>
<td>Ensures security of third-party systems that connect to an enterprise’s web applications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sygate Magellan</td>
<td>Maintains detailed information about the network’s state</td>
<td></td>
</tr>
<tr>
<td>Symantec</td>
<td>Symantec Enterprise Security Manager</td>
<td>Manages and reports on security policy compliance</td>
<td><a href="http://www.symantec.com">www.symantec.com</a></td>
</tr>
<tr>
<td></td>
<td>Symantec Enterprise Firewall</td>
<td>Provides an enterprise-level firewall for Windows and Solaris platforms</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Symantec Gateway Security</td>
<td>Integrates stateful inspection firewall, anti-virus, IDS/IPS, content filtering, IPsec VPN, and hardware-assisted encryption technologies in a self-contained device</td>
<td></td>
</tr>
</tbody>
</table>

### Network Security Summary

HP’s approach to network security begins with rigorous, widely accepted analysis and planning techniques. Network design is based on proven, integrated solutions and leading products. For organizations that must adapt rapidly, HP’s ANA technology secures enterprise networks while enabling them to change quickly in response to business imperatives.

HP and its partners offer a broad range of security expertise, products, solutions, and services to help ensure that organizations are not damaged by a disruption or compromise of their information flow. For more information, see [www.hp.com/go/security/trusted](http://www.hp.com/go/security/trusted).
Host Security

In the book *The Mezonic Agenda*, a respected security expert, Chad Davis, chases an international conspiracy to sway the U.S. presidential election. Early in the story, Chad avenges an embarrassing situation by quickly updating a very visible web page—in spite of excellent client-side security. Specifically, he discovers that Javascript validation routines in the client HTML are the sole bastion against an SQL-injection attack. He ultimately pegs down his arrogant colleague by entering:

```
'%; EXEC master..xp_cmdshell 'echo I am an Idiot! > c:\inetpub\wwwroot\home.html'
```

There are two very important—and relevant—lessons to learn from this example:

• **Security is no longer about perimeter defenses.** In the early days of mainframes, there were single points of access to computing resources and data that were easy to secure and manage. Now, however, data and processing power is distributed throughout the organization, in hundreds of different servers covering thousands or even millions of clients. There is no good place to draw the perimeter, because the network topology is so dynamic that it is generally impossible to enumerate or calculate.

• **Everybody forgets the server.** Even well-trained and experienced security architects adopt the perimeter model and neglect to recognize the inherent vulnerabilities in application and operating system (OS) code. They may also believe that platform security is not cost-effective because, unlike most other countermeasures, it requires frequent administration and introduces significant complexity into both security policy planning and security administration.

What is the point of developing a secure network perimeter with layered levels of firewalls, strong passwords, and intrusion prevention and detection systems—if a simple buffer-overflow exploit opens the web server to unfettered access by unauthorized users?

Hardened OSs have historically been hard to use, hard to integrate with the environment, and difficult to verify as secure. The most important question is whether platform security yields the expected returns. Is the effort required and total cost of ownership (TCO) too high relative to the estimated threats and the value of the assets being protected? Although platform security can be very effective, it may not always be worth the cost.

HP looked intently at this issue and enhanced the delivery of platform security through the operating environment. The result is new tools and techniques that reduce risk to the enterprise without ballooning TCO or creating an unacceptable customer/user experience. This section shares our view of platform security and its value to the overall infrastructure.

Environment

Organizations in specific sectors and industries—such as financial services, the military, and the intelligence community—have used strong platform security for decades. In the majority of other sectors or industries, the reaction to hardened OS products was a question of why an organization would want to implement them given the additional effort and inconvenience required to achieve the high level of security. This question illustrates the fact that security and platform security were not high priorities for IT administrators to warrant the cost and additional effort. In addition, as recently as ten years ago the platform security community did not differentiate between life-and-death and profit-and-loss market segments; instead, it offered a single solution to satisfy all higher security requirements.
Battlefield Protection, Enterprise Overkill

Legacy host security grows out of Cold War technology. Early offerings were based on the Compartmented Mode Workstation, an intelligence desktop that allowed secure assembly of field data gathered from spies all over the world. Correctly implemented, even the spies did not know what the data meant, because they never saw it all pieced together—hence the "compartmented" approach.

In the context of international espionage, host security was defined as:

- Separation or compartmentalization of different kinds of information
- Separation of powers or authorizations, so that nobody had all the keys
- Separation of various activities into individual tasks, each with its own associated privilege
- Highly granular accounting systems or auditing that tracked each user and system event

The main idea was compartmentalization or layering, much like the watertight compartments in a submarine: a failure in one section did not flood the entire submarine. However, transferring this security model to the connected enterprise raises some issues.

**Drawbacks of Host Security**

Host security usually has a high TCO for several reasons:

- Systems are designed for split administration (prohibiting one person from managing the whole system), which means higher personnel costs.
- The level of security usually adopts a firewall mentality: what is not expressly permitted is prohibited. That model works well for routers sorting subnets, but it breaks quickly for complex applications trying to communicate with scores of OS services over dozens of interprocess communication (IPC) connections.
- Secure platforms are often simple, functioning without today’s modern operating environment management systems. As a result, implementing routine functions requires extra effort.
- Secure platforms require custom, security-aware applications that are specifically written to behave in a way acceptable to the hardened OS.

**Benefits**

The infrastructure environment is not perfect. Ever since the early days of computing, programs have had bugs. Every piece of software contains some level of program faults, design mistakes, partially implemented features, and possible holes that developers may have been aware of but considered safe from exploit.

Layered security acknowledges upfront that systems and software always contain defects or bugs of some kind and, under the right set of circumstances, they will eventually break or be compromised. Like the proverbial submarine, military security is equipped with watertight doors, with the full expectation that one or more layers will not withstand every attack. A hardened operating environment is one of the most effective ways to prevent broken and rogue applications from violating OS security policies.

Figure 4–8 illustrates how attacks can penetrate layers of defense. If A1, A2, and A3 are attacks using different exploits, each attack is stopped at different layers in the diagram. The layered host security model assumes that bulletproof protection does not exist, and that some number of attacks will be successful. The goals are to set up several layers to prevent as many attacks as possible, survive the attacks that do occur, quickly regroup, assess and repair the damage (as possible), and continue operating as planned. Application software is often developed with the assumption that protection comes from somewhere else, and it relies on the operating environment for protection from other users/processes on the system as well as the external, distributed, and networked environment.
Commercialized Forms of Military Systems

Several attempts have been made to transition the military approach to platform security in the enterprise space. Most of these either simplify the compartment layout (preconfigured systems) or accept the requirement for ongoing, highly specialized consulting. Whether using preconfigured or customized systems, the administration costs are relatively high compared to commercial systems, meaning the TCO comparison has not traditionally been favorable. In addition, security is sometimes so tight that some applications or services simply cannot run on the transitioned systems, regardless of expenditure.

The emerging requirement expressed by HP customers is for strong host security with lower TCO, coupled with the flexibility to accommodate a broad range of applications, platforms, management tools, and markets. This led HP to analyze the host security market, along with some of our other markets, to find out whether high security can be simple, available, and cost-effective. The catch for the high-security operating environment is usually the TCO, which is generally very high when the asset value is high. However, this can be overcome if the host is chosen well, matched to the enterprise infrastructure, and surrounded by properly crafted, implemented, and enforced security policy.

Principles of Design for the Enterprise

As HP has considered how to make high security produce a higher return over a broader target market, we have made several discoveries. First, life and death situations merit a cost/benefit analysis that is different from normal business environments. The military model addresses non-financial losses, such as the loss of human life and the collapse of governments—events much more catastrophic and untenable than a simple reduction in profits. When military models are considered for business purposes, they are usually out of balance on the expense side. In other words, military security, quite appropriately, is not intended to produce a financial return on investment (ROI).

Second, these layered approaches generally assume that any manageable level of complexity is acceptable, even if the administration effort is high. This may be appropriate in a life-or-death environment. Without the military/political threat, however, the ROI is not justified, except for a few highly sensitive niche markets such as high-end financial services.
Armed with these observations, HP set out to determine whether the high-security approach can be retooled to accommodate an enterprise environment. We began to ask detailed questions about high security, exploring different aspects of military and layered security models and ways to implement these features without placing the TCO equation out of balance.

Easily Administered Layers

Regardless of how high security is implemented, layering is still needed because it is fundamental to containment and risk mitigation. It must be designed into the core operating environment to minimize tampering. Luckily, the internal mechanics are not the problem. The real issues with the military model are configuration and administration. In a typical model, compartments are defined by many layers of indirection, which leads to complexity and lack of flexibility.

In an enterprise environment, the average user depends on a specialist to define layers in most high-security platform systems. Platform layers must be simple to configure and maintain. In fact, a layered model that is both role-based and rule-based eliminates most of these administration issues, allowing the platform administrator to easily create and change configurations. If a system sets up the layering correctly and the administrator describes the layers in a straightforward way, administrative costs drop dramatically—contributing to a significant increase in ROI.

Flexible Role-Based Access Controls

It is clear that several other military security features have value in the commercial space. For example, the root account on most systems is all-powerful and able to execute any system command at any time. Even experienced administrators use root only when they require elevated privilege. This observation drives the concept of designing tools that adopt a valid role for specific commands, only for the time required to perform a specific task or function. Administrators gain privilege for each command that needs it, for the time required, and in a specific area of responsibility. These role based access controls (RBACs) can be managed on a user-by-user basis. This permits specific users to assume more powerful roles or privileges, depending on their job requirements.

Realistic Privilege Allocation and Management

Another aspect of platform security is the level of privilege assigned to system capabilities. In a true military environment, every system function has its own privilege level—much like putting lockboxes inside a locked desk drawer, inside a locked office, and so on. In the enterprise environment, there are two problems with numerous locks. First, far too many checkpoints are required for a relatively simple system operation, for example, printing a document. The extra checkpoints cause normal system operations to be slower and make applications more complex. Second, the privileges often overlap or create unnecessary redundancy.

Clearly, privileges have value in a secure environment. For example, it is valuable to control the ability to erase a disk drive or transmit files over the Internet. But the privileges must be assigned to enterprise-level activities, such as erasing a disk drive or sending files, rather than to the minute collection of system operations that make up these activities. If platform privileges are reallocated to a higher level of abstraction, they provide useful protection without incurring unnecessary costs—and thus lower the TCO.

Balanced Security and Performance

HP realized that the military model focused very little, if any, on performance. If the system did not run fast enough, more powerful hardware could be obtained. This is a critical difference between a life-or-death decision and an enterprise’s profit-and-loss decision. Espionage and battlefield situations usually involve escalation of force, little or no consideration of cost, and more and bigger hardware.
In an enterprise environment, bigger is not necessarily better or cost-effective. In fact, enterprises tend to accept a slightly higher level of risk in order to reduce costs or raise ROI. And if the security is particularly demanding of resources or effort, an enterprise might disable security features, which may be an appropriate choice for the environment. Hence, there is a need to link platform security with system performance management tools. For example, the HP-UX 11i v2 security containment and processor partitioning solutions known as vPARs (virtual partitions) and nPARs (node partitions) tie into workload management, process resource management, and the HP ServiceGuard product. (For more information, see www.hp.com/go/unix.)

In order to increase performance while maintaining security, other design goals emerge such as keeping applications in their designated compartment and preventing them from using more resources than appropriate. Another example comes from the virtual partitioning architectures: when an application needs more computing resources, it must be able to automatically add resources without compromising security. These examples of combining performance with security goals illustrate how the role of security is to support new models of operation, not to administer security for security’s sake.

Implementing Secure Platforms

Secure platforms are, to a great extent, constructed during implementation and integration. They are building blocks or foundational elements. Although not all secure platforms involve changes to the OS, most of them are so intricately involved with the OS kernel and other core operating environment functions that it is unreasonable to design a platform security system in the field. Based on that understanding, two conclusions can be drawn:

- The selection, configuration, and implementation of a solution is more important than the availability of specific security features. In other words, the security of the platform depends greatly on how it is configured and implemented.
- Because platform security is largely predesigned and configured, with little chance to redesign it for each environment, a good platform security implementation places increased emphasis on security management. A secure platform is not effective unless it is accompanied by solid security policy that supports and surrounds the platform.

This section briefly reexamines some of the fundamentals of security architecture, focusing on how they relate to implementing and assuring a secure platform.

Security Architecture Models

Unfortunately, the first step in constructing a security architecture model requires abandoning the secure perimeter model. The distributed nature of computing systems makes the perimeter difficult to locate and secure. Examining the basics of security modeling helps to understand why perimeter-based thinking is flawed. Security modeling is the fundamental baseline for security assurance, that is, for assessing and verifying the security of a given implementation.

There are probably as many security models as there are ranking experts. Examining a few of the most common models illustrates what they have in common and why the perimeter model breaks down in enterprise computing.

State Machine

State machine is the core of most security modeling and verification systems. In a state machine model, the world is divided into subjects and objects. Subjects do the acting and objects are what is acted upon. Each subject (program, process) and object (file, memory range) are assumed to have states, which change over time (state transitions).
A simple example of subjects and objects might be {man, boy, bat, ball}. Acceptable states might be {accelerating, decelerating, stationary}. Most of the acceptable state transitions would involve the boy accelerating the ball with the bat in such a way that the ball does not use the man as the unexpected subject of a deceleration state change. In a secure system, the goal is to ensure that every possible state change or state transition is considered to answer the question: if the system starts in a secure state, are there any actions of subjects on objects (state transitions) that can cause the system to become insecure?

**Bell-LaPadula**

The Bell-LaPadula model, dating from the 1970's, mirrors the classification system used by most governments to label sensitive documents. The fundamental principle of Bell-LaPadula is the way it imposes a lattice or hierarchy of subjects and objects. It facilitates a quick comparison to decide whether a given subject is allowed to perform a certain action on a given object. It hinges on proper labeling of subjects and objects, and the discussion of levels, labels, domains, and dominance can be very complex. The Bell-LaPadula model is concerned with the confidentiality of data.

**Biba**

Essentially, the Biba model is identical to the Bell-LaPadula model, except that it deals with data integrity. A user may be authorized to access certain data, but how does the user know that it is the right data and that it has not been corrupted? This model also makes use of subjects and objects.

**Clark-Wilson**

Clark-Wilson is a proxy-based integrity model, stilted toward the commercial environment and focused on separation of powers or authorizations. The goal is to prevent authorized users from making unauthorized changes to information.

**The Trusted Computing Base and Dynamic Proliferation Model**

Loosely described, the security perimeter is equivalent to the trusted computing base (TCB). The TCB is roughly defined as the set of subjects and objects over which the security administrator can have reasonable control and assurance. Things that the security administrator can cleanly identify, map, analyze, and control fall within the TCB and earn certain levels of trust. Things that are not as neatly managed fall outside the TCB and cannot be trusted (within the confines of this model).

In a perfect world, the security perimeter includes all enterprise data, users, and resources and an appropriate (reasonable or cost-effective) level of trust through various security policies and controls. Even things coming in from outside the TCB, such as network connections or anonymous customers, can be identified in a way that makes them appropriately trusted (or untrusted) subjects in a TCB state machine.

In the real world, however, this approach overlooks a problem called dynamic proliferation. Subjects and objects change state too quickly to cost-effectively maintain the TCB perimeter. The perimeter must expand and contract constantly if the enterprise is to function effectively within the business environment. With dynamic proliferation, each subject and each object must carry its own set of acceptable states, in effect forming a "mini-TCB" that must be carefully maintained. For example, a file could keep its own secure record of who can access it and what can be changed, with the record attached to the file itself and not stored in a separate database.

Currently, there are several initiatives targeted at addressing the disappearing perimeter. On the subject side, there are solutions such as federated identity management, identity and access management, and security information management. For objects, the individual repository/processing unit (the server) needs to function as an isolated TCB, which translates into the need for a secure platform.
Strategies for Implementation

Knowing the difficulties inherent in identifying and controlling the TCB, how can secure platforms be established from which to launch and manage connected enterprise services? The next few sections outline these steps.

The Confidentiality, Integrity, and Availability (CIA) Triad

All security exists to ensure exactly three things: confidentiality, integrity, and availability.

- **Confidentiality** implies no unauthorized disclosure of information.
- **Integrity** implies no unauthorized modification or destruction of information.
- **Availability** implies that authorized users can access information when it is needed.

At its most basic level, platform security selects assets that can be confined to a single server and ensures that appropriate levels of confidentiality, integrity, and availability are guaranteed for the assets while they are on that server. Assets may be data or programs, CPU cycles or bits, subjects, or objects. Security analysis usually involves a large number of security goals, threats, threat agents, exposures, risks, and countermeasures. However, the analysis circles back to ensuring some combination of these three basic properties.

Identifying Vulnerabilities

Like most security analyses, the first step in planning a secure platform is to identify the realistic vulnerabilities relative to the value of the assets being protected. Using the CIA triad is particularly helpful in this case, because it helps to quickly sort subjects and objects, and it elicits a description of useful and not-so-useful state changes.

There are three key questions for identifying vulnerabilities:

- How can the confidentiality of information on this platform be compromised?
- How can the integrity of information on this platform be compromised?
- How can the availability of information on this platform be compromised?

Answering these three questions in detail requires the security architect or consultant to address a number of other questions as part of a standard risk analysis. For example, the questions above cannot be adequately answered without asking:

- **What information** is stored on this platform? That is, what are the assets?
- **What does confidentiality** mean in this situation? Who is authorized for what information, at what time, under what conditions?
- **What does integrity** really mean? Who is authorized to change data? What internal verification mechanisms are already in place that guarantee integrity or obviously identify data integrity issues?
- **What does availability** really mean? How many users should access how much data over what time span? How often does the data change, and how quickly must those changes be propagated?

There are also inductive vulnerability assessment techniques, which involve attacking the platform in question with various exploits to see how the confidentiality, integrity, or availability of the platform might be violated. However, these must be preceded by (at least) a rudimentary paper analysis. Without knowledge of what CIA means to the enterprise, it is difficult to gauge whether a given attempt is an attack or an acceptable access method.
Identifying Threats and Threat Agents

After assessing what CIA means for a given organization or enterprise, it is useful to evaluate the threats by separating CIA into a series of common security goals, for example:

- Maintaining privacy—protecting from unlawful disclosure
- Maintaining secrecy—protecting from industrial espionage
- Maintaining integrity—keeping the data intact
- Maintaining access to service—keeping the system up and running
- Limiting abuse—defending against a malicious internal user
- Identifying problems—overcoming stealth
- Assuring security—locking out unauthorized users
- Maintaining security policy—knowing what to do, when to do it, and how to do it

For each of these areas, there are many different threats that vary in type, format, and means of attack. Rather than cataloging the threats, each of the security goals are detailed as a means for easily recognizing potential threats.

Maintaining Privacy

Privacy of data (one aspect of confidentiality) must be maintained. Certain data must be kept strictly in confidence. The risk associated with the loss of privacy is known as unlawful disclosure. Each person and enterprise should have the opportunity to choose when and with whom data is shared. In many industries, such as telecommunications and medical services, regulatory requirements and disclosure laws provide stiff civil or criminal penalties for failure to maintain the privacy of data.

Unlawful disclosure usually occurs in one of four ways:

- An authorized party (responsible for maintaining privacy) reveals information through error, neglect, or malicious intent.
- An authorized party (responsible for maintaining privacy) accidentally or deliberately grants access to an unauthorized party.
- An unauthorized party monitors communications channels (for example, a telephone tap) to obtain information while it is transmitted between authorized parties.
- An unauthorized party obtains direct access to files or other information resources to collect information.

The most common means of penetrating privacy on the Internet involves listening in on the network connection, looking for unencrypted data (cleartext), and recording it for later misuse.

Maintaining Secrecy

Access to competitive data should be limited to "need-to-know." Data is usually classified into risk categories (for example, company confidential or competition sensitive), with access to a category tied to a title or position (role). Disclosure may be unintentional or malicious. Public disclosure of secret information can mean the loss of revenue and competitive edge.

When organizations become very large, it is usually impractical to explicitly identify each person who has access to competitive information. Instead, classifications (levels of secrecy) are used. These are typically connected to job description or position in the organizational chart. This kind of security is called multi-level security because there are "need-to-know" or "safe-to-know" strata that define who can know what. All such multi-level security measures are designed to reduce the probability that sensitive data will end up in the hands of a competitor or someone who will deliberately use it to do economic damage to the enterprise.
Maintaining Access to Service

Losses can be incurred because information or computing resources are not available. Deliberately preventing legitimate access is known as *Denial of Service* (DoS). A person or enterprise should not be prevented from using information because someone else maliciously disables the means to access that information. This also applies to information resources, such as computers, networks, and communications systems. Of all threats, DoS is the most insidious and the most difficult to prevent. A simple example is someone who ties up a competitor’s telephone lines with bogus calls, preventing legitimate customers from being serviced.

One of the most common Internet DoS attacks, which can be performed by relatively unsophisticated attackers using tools available from certain web sites, involves constantly accessing (hitting) a site’s homepage, causing some customers to time out without accessing the page. If a malicious organization employed enough agents, each using a web browser to repeatedly request a competitor’s web pages, the target would be effectively closed down. Because the web pages must be available to everyone on the Internet to be effective, it is not possible to totally prevent this attack. However, effective security strategies can significantly reduce the impact and subsequent risk.

Maintaining Integrity

Deliberate corruption or destruction of data can deny access through:

- Outright destruction of files—another variety of DoS
- Overt corruption of files—data is obviously obliterated or garbled beyond usability
- Covert corruption of files—data is altered in a way that is not immediately apparent to give false impressions
- Corruption of computer programs—programs are modified to take unauthorized or destructive actions

A customer or enterprise should not be prevented from using information because someone else destroys it. This goal covers data that has been imperceptibly altered to produce bad decisions or false conclusions. It also addresses bogus programs that damage the system, including Trojan horses, viruses, and other forms of malicious code.

Limiting Abuse

Employees must not be allowed to betray trust by:

- Gaining unauthorized access to corporate data or computing resources
- Granting access to an unauthorized party
- Misusing corporate computing resources
- Corrupting or destroying computing resources

Privileged users must not be allowed to betray the trust granted to them by the organization. There are several ways that privileges can be abused. Enterprise employees may gain unauthorized access to files or corporate information systems, accessing data for which they are not entitled. They may grant unauthorized data access to a third party, such as a competitor or foreign power. They may misuse corporate computing resources to perform essential services for a competitor; or they may simply corrupt, obliterate, or steal corporate resources, as in the case of a disgruntled employee.

Unfortunately, the majority of successful penetration and espionage attempts originate inside the organization. As foreign powers once occupied with military espionage turn their efforts to economic and industrial attacks, this percentage is likely to increase. Again, as with DoS, there is no perfect defense. However, limiting employees’ access to competitive data, confidential data, and resources not required for their job (role) has a tremendous impact on mitigating this risk factor.
Identifying Problems

Identifying an attack is a cornerstone of layered security protection. Enterprises must know that a breach has occurred, identify the perpetrator and/or the means of attack (if possible), and quickly assess and control damage. Solid problem identification is the most significant step in damage control.

In spite of active security measures, there is always a probability (however small) that someone will penetrate the system. If the surveillance system is well-designed, however, the chances are high that a perpetrator will be caught or positively identified. In addition, the presence of visible surveillance often acts as a powerful deterrent to potential violators.

Even if the perpetrator is not identified and caught, enterprises must be able to assess and repair the damage as accurately as possible and repair the exploited vulnerability. This assessment is the most significant step in damage control. For example, if a corporation knows that its pricing strategies are compromised, it could change the data to confuse the perpetrator.

Assuring Security

A secure system is only part of the security solution. The system must also be configured, maintained, and operated properly. In addition, corporate procedures must support system security. Confused administrators and sloppy procedures are easy targets for attackers. To ensure that security and policy compliance is maintained, administrators must clearly understand the steps to take and the correct order. Confusion regarding the administration of a secure system often leads to inadvertent openings that a perpetrator can exploit. In addition, site security policy must ensure that hardcopy documents, media, and conversations do not reveal information being protected by the secure system. For example, positioning a computer screen to face an uncovered, first-floor window could easily defeat the purpose of all other security features.

Maintaining Security Policy

Security policy is important to the people and process part of the security equation (people + process + technology). Security policy is the set of rules and procedures for people in the organization to follow, and it also serves as a set of guidelines for process. Security policy spans how to handle information, how to conduct business transactions, what to do in the case of a security incident, and what happens when security policies are violated. To be effective, security policy maintenance must start with awareness and training, and it should continue with policy updates. All the while, documentation should also be maintained for legal and regulatory policies that require monitoring for compliance, enforcement, and investigation.

Assessing Risk and Choosing Countermeasures

Effective risk analysis for implementing a secure platform hinges heavily on the correct use of the CIA triad (discussed earlier in this chapter). It also relies on the careful and ongoing assessment of vulnerabilities, threats, threat agents, losses, exposures, and risks.

It is useful to define different types of risk-mitigation strategies that help to secure a computing platform or operating environment. In fact, there are some proven risk-mitigation strategies that help to meet the collection of platform security goals discussed previously. Furthermore, layering these strategies dramatically increases security and decreases risk. Risk-mitigation strategies include:

- Internet traffic filtering
- User authentication
- Data partitioning
- Integrity checking
- Use of least privilege
• User authorization
• System surveillance
• System alarms
• Simple security administration
• Clear site security policy, including compliance monitoring and enforcement
• Ongoing user training and awareness efforts

Internet Traffic Filtering
Stopping problem traffic before it reaches a system avoids subsequent problems and cleanup work. Filtering known bad traffic (such as virus attacks) and preventing inbound or outbound connections from/to known bad IP addresses are two examples of network traffic to stop at the outside edge of an infrastructure. A firewall is one technology that allows this type of filtering.

User Authentication
Many tools for guessing or cracking passwords are freely available. Given the low cost of powerful computers and the fact that most people choose easy to guess passwords, password cracking has become a very simple operation. To combat this, it is important to improve user authentication before granting access to resources. This can be accomplished using a combination of three authentication methods:

• **Something the user knows:** passwords that are improved to thwart cracking attempts. Password-hardening tools make users select passwords that are not comprised of common words and names.

• **Something the user has:** smart cards or physical token devices (such as a key-chain security token) can respond to a challenge during login. Users login, enter the password, and the system challenges them to enter a valid ID number (or some other credential) from the smart card or token.

• **Something the user is:** biometrics refers to measurements of unique physical features of human beings including fingerprints, retina scans, voice printing, and blood vessel printing.

There are different ways to authenticate that users are who they claim to be. Additionally, it is important to select the right level of authentication to meet security requirements and policies.

Data Partitioning
Access can be controlled by implementing a multi-level security system. Programs and users are given a clearance, and files and data are given a label. If the label does not match the clearance, access is denied. Hierarchical access can also be defined in such schemes. Multi-level security systems partition data into compartments, for example, inside (intranet) and outside (Internet). Programs running on the outside cannot access files on the inside, and vice versa. Attackers coming in from the Internet should not be able to reach into the inside compartment to access data files, run programs, or download/upload files. If programs in two or more compartments must share data, hierarchical access may be necessary. In the example given, a system compartment may be required to store configuration files and other files needed by all system programs and applications.

Integrity Checking
Security features are typically complemented with integrity checking, for example:

• Files, directories, and system tools carry security attributes.

• A master list of security attributes is maintained in a safe location.

• Files and directories are periodically checked against the list.

• If discrepancies are found, they must be explained and then fixed.
In an integrity-checking system, the system "knows" which security attributes (for example, owner, data-partitioning compartment, read access, checksum, or signature) should be assigned to key files. An administrator runs the program periodically to check the state of the file system. Any errors are immediately flagged, and the administrator can reset file attributes, restore from known good copies (if available), or disable the system until an investigation can take place.

Use of Least Privilege

In nearly every OS, programs use such OS services as terminal input/output (I/O) for portability. Normally, every program has access to every service. This unlimited access presents an opening for rogue programs and hackers. To restrict behavior, each service is protected with a privilege. If a requesting user or system has insufficient privilege(s) for access to a particular service, then that service should not be accessible. Using only the needed privilege for the shortest possible time is known as least privilege.

Every program that runs on a system must perform certain basic tasks. Because programmers do not want to recreate all of these basic operations, such as accessing files or controlling a display, the system provides a set of system services (sometimes called system calls) to handle them. Access to system services is typically unrestricted—meaning that an attacker’s malicious program could easily use system services to bypass security measures.

To overcome this weakness, system services can be divided into classes, with a specific privilege assigned to each class. All programs that expect to perform a basic operation such as I/O must present the appropriate privilege for each operation and then relinquish the privilege when it is no longer needed. For example, if a program needs to store a file, it should request write permission to the destination file system, perform the store function, and then relinquish write permission. Therefore, the program only possesses the ability to write to that file system for the time required. If the process was subsequently compromised, it would not have the ability to write.

Privileges significantly reduce the level of risk from malicious programs and Trojan horses. Because privileges must also accommodate off-the-shelf or legacy applications, there must be a special category of privileges for executable programs. However, these privileges should only be assigned by a properly authorized user within the enterprise.

User Authorization

Many systems have a superuser or root account that is all-powerful and to which all administrators have full access. Unlimited access provides an opportunity for attack. Superuser access must be divided into discrete authorizations. Every administrative job or role carries a subset of these authorizations. If defined correctly, these roles provide a balance of power.

The most common means of penetrating an HP-UX-based system is to obtain the superuser account password. If the various capabilities normally assigned to the root account are divided into discrete authorizations, each of which permit access to a very limited subset of capabilities, the superuser account can be disabled or restricted to only a few highly trusted individuals. Each discrete authorization allows access to a very small set of system features. Authorizations can be grouped into roles and distributed to specific individuals, so that users or systems have only the authorizations required to perform their specific functions. For example, night operators do not usually need superuser access to the system, but they do require certain access privileges beyond that of a normal user.

System Surveillance

There is no substitute for monitoring and surveillance. Effective monitoring and surveillance should:

- Execute at a low level, within or near the OS
- Record system events with timestamps and userids (auditing)
• Avoid degrading performance by allowing tuning and customization
• Collect and present information in real time, if possible

Because most security breaches involve stealth, the system should notify the appropriate administrators and/or security personnel when security has been breached. This allows personnel to quickly assess and limit the damage. To provide this information, the system should implement an auditing system to log suspicious activities. Since any system activity, maliciously used, could be considered suspicious, these activities must usually cover the full range of processes at the OS level. Monitoring at the system level minimizes the chances of disguising suspicious activity.

Because OS-level activities represent a very large volume of audit data, there must be a mechanism to tune resource usage, such as disk and CPU time. In addition, audit trails must often be preserved as evidence. Records management utilities must be available to allow audit data to be offloaded to and restored from removable media on a session-by-session basis. Finally, there must be post-processing tools for analyzing audit data and producing reports. Various kinds of filtering tools are needed to help focus the search for suspicious behavior.

System Alarms
Because auditing is passive, active surveillance is also needed. Effective active surveillance should:

• Execute at a low level, near the OS
• Monitor audit events or key system activities
• Filter data to allow targeting of specific events or times
• Provide real-time notification
• Activate automated defense measures
• Prioritize responses (if and as appropriate)
• Offer a high level of user configuration

Audit data must be examined carefully and the information is relatively detailed. To ease the data analysis burden and provide a real-time intrusion detection capability, systems can implement an alarm capability. Alarms can use the same set of system events recognized by the auditing feature, or they can use "pseudo-events" that address common penetration points.

Alarms may be needed for:

• Specific events that occur all the time
• Events that happen at an unexpected time of day (for example, a login at 3:00 in the morning)
• Events that happen too often (for example, five consecutive failed logins)

Alarms can also be implemented to select only certain conditions or patterns on which to trigger. When an alarm is activated, the system may do anything from simply logging the alarm to paging an operator and shutting down the system. The actions depend on the system configuration and security policy in effect at the site.

Simple Security Administration
Poor administration can nullify even the most effective security. Important attributes of security administration include:

• Security features must be simple to administer.
• Administration must be similar in format to normal operations.
• Steps must be clear and well established.
• Training of appropriate personnel should be thorough and ongoing.
• Updates to protection tools (such as patches and threat signatures) should be tested and applied in conformance with clear site security policies.

Key security features must be controllable from a native system interface, in a format consistent with the normal functionality of the system. For example, a menu-driven system should have menu-driven security controls. These controls should be divided into categories corresponding to security roles defined at the site (for example, operator, night operator, and system manager). Because maintaining a secure system can be a complex process, online help and documentation is usually essential. Each step that must be taken to ensure security must be represented in order and in a format that is easily accessible to administrators.

Clear Site Security Policies
HP has well-established processes for defining and developing security policy. It is sufficient to note some areas that are often under-addressed when dealing with platform security:

• Physical handling of media and hardcopy
• Physical access rules and procedures
• Platform security configuration control and update policies
• Handling of suspected or known penetration attempts (incident response)
• Training
• Policy compliance monitoring and enforcement

The key is to include the platform and its unique security management requirements in the overall security policy analysis.

HP Host Security Products and Solutions
HP offers a complete range of host security products and solutions to help address the threats and mitigate the risks discussed in this section. The following information provides an overview of the individual products and solutions.

HP ProtectTools for Client Device Security
Client devices tend to be the front line of access to an organization’s information assets. As such, client device security becomes a key mechanism to securing the IT infrastructure. Security requirements at the client device level can range from strengthening user authentication, to hardening the client device (at the hardware, OS, or application level), to protecting data as it resides on the device.

Client device security is of strategic importance to HP, as it is to an increasing majority of business and IT managers. As such, HP offers the comprehensive HP ProtectTools client device security solution set. ProtectTools originated with an HP developed smart card security solution for client PCs. The application is now part of HP’s business notebook and desktop smart card solutions. As the HP security portfolio has grown, the ProtectTools name has also grown to represent a broad security solution set that encompasses software, hardware, and services.

Today, HP’s Personal Systems Group (PSG) and HP Services (HPS) deliver security solutions designed to address security challenges at all levels of client devices.
HP ProtectTools for Notebook, Desktop, and Workstation PCs

The HP ProtectTools Security Manager is at the heart of the HP ProtectTools security offering for HP notebook, desktop, and workstation PCs. (See www.hp.com/go/security for product information.) This single client console application unifies the security capabilities of HP client PCs under a common architecture and single user interface. A range of features build on underlying hardware security building blocks, such as smart card technology and embedded security chips (TPMs) designed in accordance with the Trusted Computing Group (TCG) standard. Collectively, these features address business’s needs for better protection against unauthorized PC access and stronger protection for sensitive data.

Importantly, HP ProtectTools hardware security mechanisms provide the enhanced benefit of not relying solely on OS and application security vulnerabilities that are known targets to most off-the-shelf hacking tools. HP ProtectTools Security Manager embodies an extensible framework that is designed to enhance security software functionality through add-on modules. Some of these modules include:

• **HP ProtectTools Embedded Security** for strong hardware-based protection of data and digital signatures and reliable hardware-based device authentication

• **HP ProtectTools Smart Card Security Manager** for stronger user authentication, two-factor authentication mechanisms, and HP patented pre-boot authentication technology

HP ProtectTools for Microsoft Products

The HP ProtectTools for Microsoft products software suite delivers critical security enhancements to the Microsoft Windows OS, Exchange Server, and Windows Mobile platforms. Developed in collaboration with Microsoft and building on previous HP offerings called Secure Edition (SE), the new tools and services integrate seamlessly into the Microsoft infrastructure to address the needs of security-conscious organizations worldwide.

Today, the HP ProtectTools for Microsoft products solution portfolio includes a number of components:

• **HP ProtectTools Authentication Services** for enhanced protection of user passwords against various types of dictionary and other brute force attacks

• **HP ProtectTools Device Manager** for policy-driven access control to local devices such as USB flash drives and keyboards

• **HP ProtectTools E-mail Release Manager** for configurable policy support to automatically enforce use of digital signature and encryption for e-mail

• **HP ProtectTools Role Based Access** for a role based approach to more effectively managing user access rights on a large scale

• **HP ProtectTools Windows Mobile** for enhanced security for the Microsoft Windows Mobile platform providing enhanced user authentication, device access, and strong Microsoft ActiveSync authentication

With the HP ProtectTools for Microsoft products suite, HP addresses the security needs of a broader range of market segments. Customers benefit from HP security innovations that have proven reliability—the result of an exhaustive validation process in demanding customer environments.

HP NetTop™

HP NetTop™ is a highly secure and layered environment of Security-Enhanced Linux (SELinux), the VMware™ Workstation, and customized security policies. It is backed by the HP Technology Solutions Group to provide assessment, planning, policy definition, rollout, and support tailored to an organization. HP NetTop provides strong compartments that meet many government and financial industry requirements. Originally developed by the National Security Agency (NSA), HP NetTop is now offered by HP as a full-service solution to public and private enterprises.
HP NetTop Operations

To the end user, HP NetTop is simple and transparent. Users click between OS windows as they do between application windows, while the underlying NetTop works in the background with minimal performance degradation. To system administrators and their enterprise software systems, virtual machines (VMs) are indistinguishable from stand-alone workstations on the network. Applications like Microsoft Exchange, Systems Management Server (SMS), and HP OpenView work transparently with HP NetTop VMs.

Underneath, each guest OS such as Microsoft Windows executes in its own VM vault. VMs run independently from the underlying host NetTop OS; therefore, a VM crash will not affect other VMs running on the system. Since each VM is encapsulated in its own impermeable vault, data in high-assurance domains is protected against information crossover, rogue applications, malicious code, and external network attacks from other VMs and their networks.

HP NetTop Solutions

HP NetTop solutions exist for both public and private organizations. HP provides:

• **Health care organizations** with HIPAA compliance by maintaining patient records in isolated domains while allowing access to those who need it
• **Financial institutions** with customer record and financial data security
• **Defense and intelligence agencies** with Director of Central Intelligence Directive (DCID) 6/3 Protection Level 4 (PL4)-compliant, low-cost security domain separation and access to multiple coalition networks

A complete security solution—from initial assessment through rollout, training, and post-deployment support—ensures that HP NetTop works now and in the future. With HP’s unified desktop and delivery, HP NetTop adapts enterprise computing to current and emerging risks. For more information about HP NetTop, visit [www.hp.com/go/nettop](http://www.hp.com/go/nettop).

Backend Host Security Operating Systems

HP-UX

HP-UX 11i is a highly secure commercial UNIX OS that provides the fortification that e-businesses need to prevail against hacking and cyber attacks. Designed to enable Internet-based technologies and e-security, HP-UX 11i meets security requirements in the areas of policy, authorization and access control, identification and authentication, auditing and alarms, and privacy and integrity.

The 11i v1 and 11i v2 releases of HP-UX contain a rich set of standards-based and directory-enabled network security features that enable companies to build their e-businesses without compromising corporate security. These features include:

• Stack buffer overflow protection
• Security patch check
• HP-UX 11i Bastille
• HP-UX 11i Install-Time Security (ITS)
• HP-UX 11i Strong Random Number Generator
• HP-UX 11i MD5 Secure Checksum
• Networking security features such as Kerberos server, IPsec and IPfilter system firewall, AAA Server (RADIUS), Mobile AAA Server (DIAMETER), Secure Shell (SSH), directory-enablement via Lightweight Directory Access Protocol (LDAP) Services, Netscape Directory Server, and Novell eDirectory.
Microsoft

HP Services provides a number of offerings around Microsoft OS security in a client role and in the following server roles:

- Domain controller
- Dynamic Host Configuration Protocol (DHCP) server
- Windows Internet Naming Service (WINS) server
- File server
- Print server
- IIS server
- Internet Authentication Service (IAS) server
- Certificate server

These security services include configuring and hardening services, directory services, and Microsoft’s forest trust and defense in depth implementations, among many more. HP also offers exclusive Microsoft Windows 2000 Security Enhancements solutions. The solutions replace the common password hashing algorithms supplied in Windows NT and Windows 2000 with customer specific algorithms that make brute force or dictionary password hacking much more difficult.

Linux

HP provides enhanced Linux security with commitments to Common Criteria Certification, multi-level security certification through the Labeled Security Protection Profile (LSPP), and services-led security solutions. The Common Criteria Certification includes Controlled Access Protection Profile (CAPP) certification, which is increasingly necessary in government and public sector procurements worldwide. HP has completed CAPP certification at Evaluation Assurance Level (EAL) 3+, having provided verification on both Red Hat and Novell SUSE with HP ProLiant and Integrity systems. The certification includes AMD Opteron™, Intel® Pentium® and Xeon™ processor families, Carrier Grade systems, and Red Hat on workstations and laptops.

Multi-level security certification planning is underway. It will provide incremental mandatory access controls and labeling to support ultra high-level security for top-secret and ultra top-secret clearances. HP Services provides U.S. government licensed security technology in SELinux-based solutions with HP NetTop, which is discussed earlier in this chapter. Mandatory Access Control (MAC) features are incorporated into major subsystems providing effective management of multiple security levels on the desktop. For more information, see www.hp.com/go/Linux.

HP OpenVMS/Alpha Server Clusters

HP OpenVMS clusters average the fewest hours of security-related downtime as compared to key competitors. One reason for this is that HP OpenVMS was designed from the ground up as a time-sharing OS. Security was not an afterthought. In addition, HP OpenVMS clusters are relatively easy to manage and rarely require security-related patches.

Tru64

Initially, Tru64 UNIX is installed with Base Security. Upgrading the system to Enhanced Security adds the ability to implement a variety of password controls and auditing features.
HP NonStop Systems

HP NonStop systems provide strong security for a number of financial and other mission-critical applications. HP NonStop systems provide better security protection through a modular OS design, processes running in their own virtual address space, and a separation of code and data space. The systems incorporate strong encryption capability through HP’s Atalla encryption offering.

HP NonStop systems use best-practices technology to provide strong authentication, authorization, and privacy in their overall networking design. This includes support of biometrics, tokens, and PINs for authentication. Least-privilege access, role-based security, and subject/object access control models are used for authorization solutions. The HP NonStop Security Review Service provides a comprehensive assessment of the security risks to a business’s HP NonStop Server with clear, prioritized recommendations to counter those risks.

HP Atalla Security Products

HP Atalla Security Products incorporate more than three decades of cryptographic expertise and industry best practices. This enables the products to set new security, performance, and flexibility standards for increasingly sophisticated threats and escalating risks. HP Atalla Security Products provide strong Automated Teller Machine (ATM), Electronic Funds Transfer (EFT), and Point-of-Sale (POS) network security through:

- Logical security from the industry-standard Atalla Key Block cryptographic key management solution
- Physical security and performance from the Atalla Ax100 network security processors (NSPs)
- Added-value products, such as the Atalla Secure Configuration Assistant and the Atalla Resource Manager, providing flexible and unique ease-of-use features
- The Atalla Trusted Print Center and the Atalla Remote Key features, bringing robust cryptographic security to the printing of PIN mailers and the rekeying of remote ATMs
- Broad support of leading financial institutions, independent software vendors (ISVs), and HP financial industry partners

For more information about the HP products discussed above, see www.hp.com/go/security/trusted.

Host Security Summary

Host security has traditionally been a military-grade solution with high costs in the areas of user satisfaction, user productivity, and operations—in addition to the cost of the solutions themselves. Host security is transforming to meet the needs of businesses and other organizations, which are driving secure hosts to deliver ease of administration, flexible role-based access control, useful privilege management, and security balanced with performance.

The concept of relying solely on a bulletproof perimeter defense is evolving into the concept of layered defenses that acknowledge the real threat environment. Furthermore, the layers need to extend all the way down to the servers themselves. The motivation for these changes comes from far-reaching, global virus attacks, such as the Blaster and Sasser worms, that have easily crossed secured perimeters.

HP has intently examined the issues related to host security to enhance the delivery of platform security through the operating environment. The results are new tools and techniques that reduce the risk to enterprises without ballooning TCO or creating an unacceptable customer or user experience.
Storage Security

In principle, storage security is straightforward. In practice, establishing storage security requires specialized knowledge, careful attention to detail, and ongoing review to ensure that storage solutions continue to meet an organization’s evolving needs. Most importantly, security by its nature is a three-way balance between the cost of the security measures taken, the impact of a breach, and the level of resources a determined intruder needs to overcome the security measures.

Environment

Storage security represents a major component of the overall security plan for a data center and a business. Consequently, business policies and practices must augment any hardware- or software-level security model, including network and system security.

Threats

Storage has evolved into a resource shared by many systems on a network. In many cases, it is no longer sufficient to secure just one system to which a storage device connects, because storage devices now connect to many systems. To protect against a variety of threats (not all of which can be anticipated in advance), storage security must address the varying security requirements of a diverse number of databases and applications. For example, storage security must protect:

• Valuable data belonging to each system against unauthorized access, modification, or destruction by any of the other systems
• Storage devices themselves against unauthorized configuration changes, with audit trails of all such changes

There is no value in carefully securing storage and subsequently leaving the system wide open to the Internet. Storage security must be a part of an overall security plan, both for a single data center and for the organization as a whole. Storage security is also a set of procedures that define access rights for data and authority for managing devices, and it defines an appropriate response when security issues occur.

Types of Storage

There are three main types of storage to consider today and two emerging technologies:

• Direct Attached Storage (DAS) is connected directly to a single system, similar to the disk within a PC.
• Network Attached Storage (NAS) is accessed via the Ethernet LAN network, and it stores and retrieves files.
• Storage Area Network (SAN) storage is accessed over a storage network, which today is typically Fibre Channel architecture, providing what looks like disk drives to systems.
• Internet SCSI (iSCSI) offers storage networking over IP networks, but it is not yet in widespread use. iSCSI is an important addition to SAN technology because it enables a SAN to be deployed in a LAN, WAN, or MAN (local-, wide-, or metropolitan-area network).
• Object storage is an emerging technology that combines aspects of SAN and NAS.

HP’s storage security focus is on storage shared between many systems on a network, primarily SAN and secondarily NAS. Storage security is not a box added to a SAN as a firewall is added to a network. Security must be an attribute of every system, every switch, and every device in the SAN.
Benefits

Storage security provides protection from attacks and resulting exposures. Specifically, storage security:

• Protects data confidentiality
• Protects data integrity
• Protects data from destruction or loss

Principles of Risk Mitigation

Many ways exist to gain unauthorized access to data and to retrieve, alter, or destroy data. Examples of risks that may require mitigation include:

• Stealing disk(s) and backup tapes
• Copying disks
• Allowing an unauthorized system to access a disk array or tape library
• Wiretapping within a data center and between data centers
• Making unauthorized changes to permissions in the disk array or in the switch
• System mounting and initializing a volume it does not own as a result of a software defect
• Operator error or miscommunication

Mitigation Techniques

Mitigation of storage security risks involves identification and authentication, authorization, auditing, and encryption.

Identification and authentication techniques include:

• User logon identification and authentication via security mechanisms such as user name and password protection for authorization of administrative actions
• Audit trails (logs) to identify what was done and by whom, which deters deliberate misuse of authority and helps recover from incorrect actions
• Timely revocation of an individual’s identity or modification of authorization when responsibilities change or the individual leaves the organization
• Device identification and authentication through emerging technologies that ensure a device is permitted on the storage network (These technologies can also detect an “impostor” rogue device pretending to be a different device or system.)

Authorization techniques include:

• Authorization for an individual to manage only specific devices or to limit access to many devices
• Verification by storage devices that an administrator who issued a command is authorized to do so, before performing the requested action
• Verification by disk arrays that the specific system that issued a read or write command has permission to do so for that Logical Unit Number (LUN), before performing the input/output (I/O) action (Through emerging technologies, a tape library controller can similarly verify permissions on I/Os to a tape library.)
Auditing techniques include:

- Logging all administrative actions (changes) and any significant events (This is typically logged individually within devices, but logging software is the preferred method because it presents a single view and allows queries.)
- Extending the auditing mechanism over the entire storage network to track activities related to each element

Encryption techniques include:

- Encrypting data on media such as a disk or a tape
- Encrypting data “in flight” between data centers (and potentially within a data center) to protect against wiretapping

Encryption will gain more widespread use over time. Encrypting and decrypting data at hundreds of megabytes per second (storage system speed) is considerably more difficult than encrypting a few thousand bytes using software on a PC. In the security domain for storage, data copied between data centers is no longer protected from wiretapping by the physical security of the data centers. The lack of physical security on cables outside the data center can be mitigated by passing the traffic through a dedicated encryption system before it leaves the sending data center.

Dedicated encryption systems are available for both Fibre Channel and IP networking, with the latter called Internet Protocol Security (IPsec) gateways. Because of the cost and complexity, such installations are not as common today. In the case of iSCSI, HP anticipates that IPsec will be built into future interfaces, making encryption more affordable and more ubiquitous than is currently possible with IPsec gateways.

Data Access and Management Measures

Mitigation approaches generally fall into data access measures and management measures. Figure 4–9 categorizes these mitigation approaches by data security and management security.

Data access approaches include device authentication, device authorization, and encryption. Management techniques include individual authentication and authorization, with audit trails and logging. Some of the items in these categories are routinely used today. Others represent evolving, leading-edge mitigations.
Secure Storage Priorities

As businesses set secure storage priorities for the coming years, securing the management interfaces of all devices is usually the highest priority. The key priorities for storage security include:

- Facilitating secure management of ports and interfaces on elements such as switches and arrays by:
  - Using strong passwords and changing default passwords
  - Disabling unused management ports on devices
  - Enabling firewall management of LAN interfaces to block widespread access
- Enabling LUN security (for example, Selective Storage Presentation and LUN Masking) if applicable
- Using encryption, if warranted to meet specific business objectives

A plan for storage security must incorporate people and procedures as well as equipment. It must fit with the overall data center and business plans. This means evolving the plan as both the situation and technology allow, training users accordingly, following the plan, and testing it.

Storage Security Summary

Storage security is part of HP’s Trusted Infrastructure and is a major component of the overall security solution. Storage plays an indirect but critical role in an enterprise’s overall security operations. A data center contains the majority of an organization’s records; many business processes are affected if storage systems become unavailable or are compromised. An organization’s storage and storage security strategy must relate directly to the business processes, IT infrastructure, and overall security model of the organization. Storage security draws not just on the organization’s security governance and attitude toward risk, which is driven from a business level, but also on its centralized identity (authentication) and authorization services and its security management capabilities for managing threats.

In addition to mitigating security risks through independent identification, authorization, auditing, and encryption techniques tied to storage, a broader plan for infrastructure security across storage, networking, and hosts must also be in place. An attacker will seek weaknesses across all three areas. Securing storage over standard networking depends on how effectively the network is protected and on the security of the storage system itself. This is particularly true when storage is accessed over the organization’s backbone network rather than through an isolated storage network or subnet.

HP Trusted Infrastructure Services

HP offers a wide range of services capability for designing and implementing trusted infrastructures that meet customer’s business needs. HP’s Consulting and Integration Services combined with HP Technical Support and HP Managed Services offer trusted infrastructure services at every point in the security life cycle.

The following is an overview of HP’s Trusted Infrastructure services (see www.hp.com/go/security):

- Infrastructure review and implementation design
- Security assessments across the infrastructure
- Physical asset protection
- Network, system, and host security
- Adaptive Network Architecture
- Application security and application auditing
- Security workshops and training
Trusted Infrastructure Summary

As reliance on IT infrastructures increases for businesses and society, we face important challenges. We must stay ahead of the security needs for reliable infrastructure technologies. Fundamental IT building blocks must be innovated and redesigned to include security features. From clients to servers, from networking to storage, and in printing technologies, infrastructure security mechanisms must be continually improved to support adaptive and flexible IT solutions.

HP is investing to ensure that we continue to deploy secure and reliable trusted infrastructures. HP is an industry leader, driving this agenda across platforms, OSs, and infrastructure solutions. Importantly, HP’s leadership in the TCG has brought the industry together to greatly increase baseline security of infrastructure technologies to meet current and future customer needs.

Alongside other efforts, such as establishing secure development practices within HP and driving infrastructure technology standards, Trusted Computing provides the security building blocks that allow the IT industry to continue to innovate and deliver the power of IT across reliable trusted infrastructures.

Table 4–4
HP Trusted Infrastructure Solution Offering Summary

<table>
<thead>
<tr>
<th>Solution</th>
<th>TI Focus Area</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Virus Throttle</td>
<td></td>
<td><a href="http://www.hp.com/go/procurve">Click Security</a></td>
</tr>
<tr>
<td>HP Adaptive Network Architecture</td>
<td></td>
<td><a href="http://www.hp.com/go/services">Click Adaptive Network Architecture</a></td>
</tr>
<tr>
<td>HP Active Countermeasures Service</td>
<td></td>
<td>Contact HP</td>
</tr>
<tr>
<td>HP/UX 11i</td>
<td></td>
<td><a href="http://www.hp.com/go/unix">Click Security (under HP/UX 11i Capabilities)</a></td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td><a href="http://www.hp.com/go/Linux">Click Security</a></td>
</tr>
<tr>
<td>HP NetTop</td>
<td></td>
<td><a href="http://www.hp.com/go/nettop">www.hp.com/go/nettop</a></td>
</tr>
<tr>
<td>HP OpenVMS/Alpha Server Clusters</td>
<td></td>
<td><a href="http://www.hp.com/go/openvms">www.hp.com/go/openvms</a></td>
</tr>
<tr>
<td>Tru64</td>
<td></td>
<td><a href="http://www.hp.com/go/tru64unix">www.hp.com/go/tru64unix</a></td>
</tr>
<tr>
<td>HP NonStop Systems</td>
<td></td>
<td><a href="http://www.hp.com/go/nonstop">www.hp.com/go/nonstop</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td><a href="http://www.hp.com/go/security">Click on Security Services (under Featured Products and Services)</a></td>
</tr>
</tbody>
</table>
For additional information, refer to the following resources:


- Cisco's documentation web page: [www.cisco.com/univercd/home/home.htm](http://www.cisco.com/univercd/home/home.htm) (For general references, see the links under the "Hot Items" and "Networking Information" headings.)

- SANS Institute Information Security Reading Room: [www.sans.org/rr/](http://www.sans.org/rr/) (An excellent selection of white papers on a wide variety of network and general security topics.)


Chapter 5 Conclusion

"HP's strategy is to build security into its products, drive industry standards on security and privacy, align business and regulatory requirements with security life cycle delivery, and innovate ways to deliver a safer IT environment for our customers."

—Tony Redmond, Vice President and Chief Technology Officer, HP Services
Inventive, Reliable Security

All of HP’s businesses sell products, services, or solutions that require varying levels of security, both to be acceptable to customers and competitive in the market. Security is increasingly becoming an attribute that is associated with quality. HP wants our products, services, and solutions to be secure in operation, deployment, and use. We want to be known as a company that designs for security and privacy, drives best practices, contributes in a significant manner to new security standards, and delivers a safer IT environment to our customers. We draw on our own resources as well as those of our pure-play security partners, such as Symantec, Check Point, Sygate, Nokia, Cisco Systems, and VeriSign, to deliver hardware and software products and services that contribute to our strategy and meet the requirements of our customers.

Figure 5–1
HP’s Security Framework

Delivering a safer IT environment requires a framework for rapid and effective response to threats and business objectives. HP focuses on the key areas of governance, identity management, proactive security management, and trusted infrastructure to bring our customers the safe, proactive, and adaptable IT environment that is necessary to support the objectives of companies and organizations today and in the future.

Governance

HP’s Security Governance Services provide companies and organizations with an enterprise-wide policy foundation, a governance model, and an organizational structure. The program can apply to the entire enterprise or to a business line, and it defines the integration and orchestration principles that shape the enterprise security system. This program meets the requirements of the ecosystem in which the enterprise operates, including regulations, business community practices, technology constraints, and the culture specific to the enterprise. Security governance provides guidance on how IT staff translates business security requirements into security measures and implementations. HP’s Security Governance offering includes risk mitigation, security strategy and policy services, security training and awareness, security architecture, monitoring, and threat and vulnerability assessment.
Identity Management

HP is pursuing a pervasive identity management framework—extending beyond conventional enterprise applications to encompass a wide range of intelligent devices that provide individuals with a vastly simplified experience. By playing a leadership role in driving standards organizations such as the Liberty Alliance, HP is deeply committed to being at the forefront of the next-generation federated environment. Federated identity management systems reduce the difficulty of creating and maintaining secure business collaborations, and they simplify the interactions that consumers have with electronic enterprises by reducing the number of digital identities that they must possess and manage.

Identity management systems can authoritatively identify with whom and what (systems) we interact, their characteristics, and the level of permissions or restrictions in terms of information access and privacy. In addition, we can do this in an efficient way—anywhere, anytime, and by a variety of means. HP delivers identity management services based on its own software (for example, HP OpenView Select Access and HP OpenView Select Identity) and partner offerings that integrate with the major enterprise directories such as Microsoft® Active Directory and Sun Java System Directory Server.

Although HP delivers federated identity solutions for enterprises today through techniques such as intelligent provisioning and single sign-on across multiple platforms, attaining true federated identity between enterprises is only possible through adherence to well-crafted and widely adopted standards. HP therefore works with industry initiatives such as the Liberty Alliance to represent and advance the interests of HP and our customers and enable federated identity management across multiple platforms, applications, and communities.

HP considers identity management in a variety of contexts to help enterprises:

- Manage their internal user population for enterprise applications
- Manage mediated applications that use web services
- Provide access and manage identity information for customers and partners
- Collaborate in federations to provide a simplified experience and the necessary security to customers and partners

HP's vision is to enable the Adaptive Enterprise with complete federated identity life cycle management solutions. HP OpenView Identity Management puts control in the hands of the business user with a suite of scalable applications focused on ease of use, expedited deployment, and the ability to embrace change. To that end, HP has many offerings available today and future plans to provide an end-to-end identity management solution.

Proactive Security Management

Although we can continue to bolster the battlements of strong network defenses, the increasing pressure applied to these defenses has caused them to leak. Other issues that cause viruses and worms to penetrate defenses include human frailties that result in errors in system configurations, available patches that are not applied, and mismanagement of computer resources. HP’s strong belief is that the security industry must move from its historically reactive approach to a much more proactive stance.

Traditionally, the focus has been on erecting strong perimeter defenses by deploying firewalls, demilitarized zones (DMZs), and intrusion detection, anti-spam, anti-virus, and other systems. This approach has served the IT industry reasonably well in the past; however, the increasing threat velocity and sophistication we see today threaten to overwhelm these defenses and presents a strong argument for a more coordinated, integrated, and enterprise-wide response. In effect, we have created a hard shell around our IT infrastructures and a vulnerable soft center that is open to worms and viruses. Given the ever-increasing number of threats that affect the Internet, a shift in approach is of growing interest to our customers.
Today, there are more attacks than ever before. System administrators have less time to learn about new vulnerabilities and test and apply patches before attackers attempt to exploit them. And if an attack gets through the perimeter, it can spread faster than human beings can manage the infection. These facts have driven HP to move our interest and R&D activities away from reactive security management to a proactive approach for protecting IT infrastructures. System administrators are already under time pressure; the most logical approach is to build more intelligence into computers and network components so that they can recognize and respond to threats.

HP’s Active Countermeasures technology can scan huge IP networks for vulnerable systems and mitigate the problems. HP’s Virus Throttle technology can detect abnormal network behavior of the same type that a propagating virus often exhibits and then limit network connections to choke the ability of the virus to continue spreading. Integrated with a comprehensive incident management system (a consulting service available from HP Services), these technologies help companies protect the soft center of the IT infrastructure within a strong perimeter.

Proactive security management has the capability to protect data, applications, systems, and networks in the face of rapidly changing threat environments and changing business models. Proactive security management enables the vision of HP’s Adaptive Enterprise by delivering policy-driven security management across the enterprise to prevent, detect, warn, log, and heal the effects of attacks, security policy violations, and other threats. Our work to develop innovative solutions such as Active Countermeasures and Virus Throttle establishes the basis for helping customers resist the flood of threats to internal and external networks today—threats that now spread at computational speed.

HP’s Proactive Security Management strategy evaluates the security environment and responds to changing conditions. HP Services, HP IT, and HP Labs are cooperating to commercialize the techniques used within HP’s own network to proactively detect and repel threats. This experience has driven us to develop a comprehensive incident management program and a security policy-driven event management system that are incorporated in the OpenView branded product suite. In addition, HP drives programs to deliver security patch management, policy management, and auditing and accounting in an appropriate manner for each of our customer segments so that users can trust the platforms on which they rely.

**Trusted Infrastructure**

At the host platform level, trusted infrastructures address the problem of devices we deem to be untrustworthy, such as the PC. The PC is untrustworthy because its basic architecture emerged at a time when threats did not exist to the degree of virulence that we know today. HP’s approach is to work with other industry partners to set new standards for platforms, operating systems (OSs), and applications that create the building blocks that underpin truly trusted infrastructures. HP’s strategic effort to drive industry standards in this space includes its work through the Trusted Computing Group (TCG).

At the network level, conventional network-perimeter defense systems cannot simultaneously meet the need for business agility and the need for protection of information assets. To enable connectivity to business partners, for example, system administrators must frequently manage network firewalls with ever-growing lists of exceptions. This process is both clumsy and prone to errors, and it requires a new set of approaches for the design of network security architectures. HP is responding in a variety of ways. HP’s Adaptive Network Architecture (ANA) is one answer to the network agility and security requirements of today’s businesses; it provides a compartmentalized, network-access policy management system and security architecture. More generally, HP plays a leadership role by working to establish effective network security standards, such as IEEE 802.1X, and participating in the Trusted Network Connect (TNC) working group of the TCG organization.

Trusted platforms are only one building block towards attaining a secure infrastructure and computing environment. They form the basis for Trusted Solutions and Trusted Ecosystems—future systems that deal with use cases that today’s untrustworthy infrastructure cannot handle. Trusted platforms and networks
do not create or make security, but they do make it easier for customers to achieve truly dependable infrastructures. Trusted platforms help form the basis for ad hoc, interoperable-trust frameworks, with secure interoperability from mobile devices to enterprise data centers, across heterogeneous hardware platforms and OSs. They help protect data, applications, and infrastructures against unauthorized access and enable trustworthy use models.

HP’s Trusted Infrastructure strategy encompasses the design of inter- and intra-enterprise security solutions. It is a combination of system, device, storage, and network security capabilities built into our offerings to protect the availability, integrity, and confidentiality of data and processes.

HP Labs Invention

HP Labs security research contributes innovative technology breakthroughs across all aspects of the corporate security strategy. Focused research aligns directly with primary initiatives and drives business units to think differently about approaches to security challenges. Innovation for the short term focuses on protecting the soft center of networks and systems (behind the perimeter) by incorporating more intelligence in hardware and software so that these components can better detect and resist attacks. Virus Throttle and Active Countermeasures are good examples of innovations that HP employs within its own infrastructure and is transitioning to customer offerings. In addition, HP Labs invests in longer-term research to sustain a competitive pipeline of invention and innovative security capabilities for a wide range of emerging technology and application domains.

Proactive Security for a Safer IT Environment

Today’s enterprise environment is increasingly volatile due to changes driven by business opportunity and threats emerging from attacks that are ever more sophisticated. In addition, government regulation is increasing corporate accountability for proper business practices and for protecting individual privacy. These pressures mandate a change in tactics for IT security—a change to a new proactive approach rather than the conventional reactive approach.

To enable our customers to implement a proactive IT security environment, HP wants our products, services, and solutions to be secure throughout their life cycle. By focusing on the key areas of identity management, proactive security management, and trusted infrastructure with keen attention to governance issues, we have developed a solid framework for proactive enterprise security. With this framework, we deliver a safer IT environment to our customers—one that responds to changes in threats and corporate business objectives while it maintains defined levels of security and risk.
Appendix A

Principles of Design for Network Security

Standardization

Each type of network component, design, procedure, or baseline configuration has its own security implications. Each of these elements must be consistently managed and periodically reviewed as an organization evolves and its threat environment changes. Therefore, reducing the number of dissimilar elements in the network environment will, in general, reduce the complexity and cost of security.

For example, reducing the number of different operating system (OS) platforms reduces the number of job descriptions, operational procedures, administrative tools, and other supporting elements for which an organization must train users, identify threats, assess risks and vulnerabilities, and implement countermeasures. Furthermore, standardization of job descriptions, required training, and local team organization can significantly simplify security management.

Another advantage of standardization is the ability to deploy widely tested and trusted approaches throughout the enterprise. For example, standard protocols for secure communication such as Secure Sockets Layer (SSL), Secure Shell (SSH), and the IPsec (IP security) protocol family have been widely scrutinized and, over time, strengthened against a wide variety of potential attacks. By standardizing on a limited number of well-accepted technical approaches and business best practices, organizations benefit from the experience and efforts of countless contributors over many years.

In some cases, however, implementation of diverse countermeasures (such as Linux-based bastion hosts to further secure a properly configured Microsoft® Exchange e-mail infrastructure) can provide additional protection that outweighs the additional complexity. Therefore, the advantages of standardization should be balanced, in some instances, with the advantages of diverse countermeasures as part of a layered defense strategy.

Likewise, standardization brings with it an increasing requirement that whatever is standardized must be highly secure. A single vulnerability exploit can affect the entire network. Appropriate standardization can, however, conserve resources that can be applied to diverse countermeasures. For example, an organization could standardize on a regional e-mail infrastructure based on specific Microsoft Exchange and bastion host configurations.

Least Privilege Access

Individuals, systems, applications, and business processes should have access to the minimum amount of information necessary to conduct business. Least privilege access depends on the existence of a robust means of establishing and managing digital identities. (For more information about digital identities, see the Identity Management chapter.)

Least privilege access for networks has broad implications. It means that only public network resources should be available to individuals whose identity or organizational affiliation is unknown or unauthenticated. Individuals who must access the network, including individual network hosts, should only have access to the network-related information and equipment they need to do their job.

For example, operations personnel should not have access to application source code, and application developers should not have access to the resources needed for actively managing the production network. Physical access to data centers, telecom cabinets, and other network equipment should be restricted to authorized individuals.
Least privilege access involves more than people. An attacker could compromise any network resource. Resource privileges, and the privileges available through them, should be restricted to the minimum necessary to meet business requirements. For example, router access control lists (ACLs) and firewall configurations should be as restrictive as possible. Unnecessary services should be shut down on servers. Public resources such as web servers should be carefully secured to prevent unauthorized manipulation by external attackers.

Finally, least privilege access also involves the distribution of network traffic. IP networks are inherently insecure. Any wired or wireless network is a potential target for attackers seeking to observe or alter network traffic. On a LAN without switches, each datagram (message or message portion) reaches all host network interfaces, and it is up to the host to determine how the datagram is processed.

Encryption of sensitive information is an important countermeasure. All sensitive (non-public) information transmitted over wireless networks or the Internet should be encrypted. Encryption may also be applied to data stored on or transmitted over internal networks. However, encryption is not always feasible, and most encrypted network traffic remains susceptible to the analysis of communication patterns between network hosts, which is known as traffic analysis. In addition, if traffic from public network resources competes for bandwidth with internal network traffic, the organization is susceptible to a crippling Denial of Service (DoS) attack launched through the Internet.

In summary, traffic should not flow over a network segment unless there is a business need. Switches, which are commonly used to improve network performance, can also improve network security by channeling network traffic directly to its intended recipient or to a small subnet. Network designers can also use Virtual LANs (VLANs)—which define network membership on a logical basis rather than a physical basis—to resegment networks without rewiring them. Therefore, network designers can partition hosts and host traffic based on business and security requirements rather than physical location. Together, switches and VLANs can help prevent unnecessary distribution and exposure of network traffic.

Layered Defense

A layered defense is essential to an enterprise’s network security strategy, approach, and implementations. Such an approach includes appropriate security policies, security awareness and training, security technology, best practices implementation and operation, and auditing.

Technology is critical to any layered defense strategy. An enterprise would not consciously connect internal networks to the Internet without a perimeter defense mechanism such as a firewall. However, even firewalls cannot be relied upon as the only way of protecting the network. Technology must be layered to provide maximum coverage and security for an enterprise’s information assets.

The principal layers of security technology represent the perimeter, network, and hosts. Thus, in addition to a network-based Intrusion Detection System (IDS), a host-based IDS should be used to ensure host integrity. Encryption, anti-virus, system auditing and logging, backups, honeypots (hosts or other resources such as decoy user accounts used to lure and observe attackers), and other technologies support a layered defense strategy. Building a layered defense strategy requires breaking networks into divisions such as subnets and demilitarized zones (DMZs), with multiple layers of screening routers, firewalls, virtual private network (VPN) deployments, anti-virus solutions, intrusion prevention systems (IPSs), and IDSs to help identify malicious traffic not prevented by perimeter defenses.

Countermeasures must be combined to be effective. Any single countermeasure could fail or be susceptible to an attack, now or in the future. Similar to least privilege access, layered defense has broad applications to network security. For example, to log on to a system designed for internal use in a well-secured network, an attacker must penetrate multiple firewalls and routers secured with ACLs and somehow obtain a valid access credential. In addition, an IDS/IPS plays a role in mitigating the risk of unauthorized system access. If the attacker is a curious visitor who has obtained a valid user name and
password by looking over an employee’s shoulder, other controls must also be in place. These controls typically include site physical security, security policies, and awareness programs that shape employee behavior as well as logging and auditing of access to sensitive resources.

There are other important examples of the need for a layered defense. For instance, an employee downloading malicious software during an SSL browser session can circumvent many layers of classical network defenses such as firewalls and IDSs; consequently, additional defenses are necessary. These defenses typically include employee awareness efforts and policies against misuse of company resources as well as the enforced presence of personal firewalls and updated anti-virus software.

Network designers should think of a layered defense in three ways:

• Layers of different approaches that span physical, technical, and administrative controls
• Layers of physical and technical obstacles that a potential attacker must overcome
• Layers of countermeasures that prevent attacks, detect and report attacks, limit the damage that a single attack can carry out, and facilitate recovery from attacks

Redundancy

The network designer must consider the enterprise-wide impact of the failure or compromise of any network component. Redundant service providers, connections, entry points, and network services should all be considered. However, redundancy makes networks more complex and expensive. Therefore, it must be carefully justified. For example, redundancy may not be justified for a reliable switch that services a small workgroup, but Internet access for a major campus may well warrant redundant connections from different service providers.

Compartmentalization

Enterprise networks can be divided into compartments or subnets to control security and other operational risks, facilitate standardization, establish least privilege access, and achieve a degree of redundancy. Many organizations use the structure of their business operations as an initial guide to compartmentalization. For example, if an organization is partitioned into three major divisions and a corporate office, four business application compartments may be warranted.

One of the advantages of compartmentalization is that access policies can be determined centrally and implemented at compartment boundaries. In the example network of four business application compartments, hosts in each compartment may have limited access to hosts in other compartments because each division operates independently. However, hosts in the corporate network may have more extensive access to the divisional compartments to enable integration and oversight of divisional operations.

In addition to business application compartments, compartments can be created for other purposes. As shown in Figure A–1, compartments for cross-business services might be created by grouping e-mail, directories, and naming services; tools to monitor and manage the network; and all end-user desktops
in separate compartments. Other compartments may contain applications that are accessible from the Internet (such as corporate and divisional web sites) and hosts that are accessible to external organizations and individuals via secure remote access. Compartmental access policies generally allow most types of outbound traffic, but they limit inbound traffic based on business need or application type.

Compartmentalization facilitates adoption of other design principles, for example:

- Standardization is facilitated by centralizing policy management and providing standard network topologies for particular purposes.
- Least privilege access implementation is simplified by compartment access policies.
- Layered defense is facilitated by secured compartment boundaries that provide an additional layer of defense between the host and the network perimeter.
- Redundancy principles can be addressed by redundant resources implemented within the same compartment but at different physical locations. Multiple network routes may be established between compartment partitions located at different sites. Compartments themselves may be connected with a virtual backbone composed of redundant network routes.
Appendix B

Virtual Private Network (VPN) Technologies

This appendix discusses the three virtual private network (VPN) technologies as specified by the VPN Consortium (VPNC; www.vpnc.org), the international trade organization for manufacturers in the VPN market:

• IP security (IPsec) with encryption in either tunnel or transport modes
• IPsec over Layer 2 Tunneling Protocol (L2TP)
• Secure Sockets Layer (SSL) 3.0 or Transport Layer Security (TLS) with encryption

According to the VPNC, all traffic on a secure VPN must be encrypted and authenticated, the security properties of the VPN must be agreed to by all VPN participants, and no one outside the VPN can affect the security properties of the VPN. In addition, an administrator who knows the extent of the VPN must control secure VPNs.

Note that TLS is a successor to SSL. Like SSL, TLS provides client and server authentication along with message privacy and integrity. Although SSL and TLS are not identical, TLS contains a mechanism for backward compatibility with SSL 3.0. Furthermore, the two protocols are similar enough that only SSL VPNs will be mentioned further in this discussion.

IPsec With Encryption

IPsec is a standard security protocol defined by the Internet Engineering Task Force (IETF). IPsec provides network-level access control, connectionless integrity, data origin authentication, and data confidentiality services.

Protocols

IPsec uses three protocols to provide services. The Authentication Header (AH) protocol provides authentication and data integrity services but not encryption. The Encapsulating Security Payload (ESP) protocol provides encryption and authentication services. AH and ESP can be used separately or in combination. The Internet Key Exchange (IKE) protocol determines the encryption and/or authentication services to use.

IPsec supports authentication using a shared secret key or X.509 digital certificate, also known as a public-key certificate. IKE also manages distributing and updating the symmetric (shared) encryption keys used by ESP. When exchanging keys, IKE can use the Diffie-Hellman method, which enables exchange of cryptographic keys between two parties in a manner that cannot be compromised by an attacker and does not depend on previously shared keys. Secure use of Diffie-Hellman key exchange, however, still requires prior confirmation of the identities of both VPN endpoints.

IPsec is extremely flexible and it can be implemented in a number of different ways to provide authentication data integrity, confidentiality, key management, application transparency, and session management.

Modes of Operation

IPsec defines two modes of operation: transport mode and tunnel mode. Transport mode is for end-to-end communication, and the original IP header is not encrypted. Tunnel mode is for communication between a set of gateways interposed between the communicating hosts. At each gateway, a new IP
header is added and the entire original packet is encrypted. Tunnel mode is more secure than transport mode because it conceals the identity of the sending and receiving hosts. Using these two modes, IPsec can support a variety of communication links (Figure B–1).

### Figure B–1
Types of IPsec Communication Links

**Host-to-Host Topology**

**Host-to-Gateway (VPN) Topology**

**Host-to-Host Tunnel**

**Gateway-to-Gateway Topology**

---

**IPsec Over L2TP**

IPsec over L2TP provides the security advantages of IPsec (above) on non-IP networks. L2TP is a Point-to-Point Protocol (PPP) extension to enable operation of VPNs over the Internet. Unlike IPsec VPNs that work on the network layer and require IP, L2TP works at the data link layer and is protocol independent. It combines the best features of two existing tunneling protocols: the Microsoft® Point-to-Point Tunneling Protocol (PPTP) and the Cisco Layer 2 Forwarding (L2F) protocol.

**SSL VPN**

Unlike the well-established IPsec and L2TP-based VPN technologies, SSL VPN is a relatively new but increasingly mature technology for securing remote access to enterprise resources and data. SSL VPN-enabled applications run within SSL sessions and use application-level reverse proxies to connect external users with internal servers. Although SSL is standardized, SSL VPN implementations differ between vendors—especially in the way they support access to backend applications and data.

Because they operate at the application level, SSL VPNs can enable access control with finer granularity than network- or link-level VPNs. Therefore, SSL VPN can track more information about users and applications. SSL VPN is also popular because it can use a web browser as a client, often with a
plug-in or helper application. In fact, SSL VPNs are sometimes referred to as "clientless VPNs" because they leverage the client web browser. This is particularly important for small devices, such as PDAs and cell phones, which may not have sufficient resources to participate in other types of VPNs. Furthermore, since SSL and application-level proxies work above the transport layer, they are not affected by network address translation (NAT) issues, which are increasingly common and often conflict with IPsec VPNs.

It should be noted that many intranets do not allow outbound host-to-host or host-to-gateway VPNs, due in part to a reluctance to leave the required ports open to Internet access. However, nearly all intranets allow outbound SSL sessions due to the ubiquitous need to enable secure access to external web sites.

On the other hand, unlike IPsec's application transparency, not all applications work with SSL VPN. The applications must be developed with SSL support, or they must work with proxies or specialized client-side software. Because of these and other reasons, different SSL VPN products work with different applications. Successful implementation depends on careful planning and testing prior to product selection.

Table B–1 summarizes the VPN technologies discussed, including their advantages and disadvantages.

<table>
<thead>
<tr>
<th>Type</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPsec with encryption</td>
<td>• Extremely flexible</td>
<td>• IP networks only</td>
</tr>
<tr>
<td></td>
<td>• Several ways to implement</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Application transparent</td>
<td></td>
</tr>
<tr>
<td>IPsec over L2TP</td>
<td>• Protocol independent</td>
<td>• Must use IPsec over L2TP (L2TP does not provide security mechanisms)</td>
</tr>
<tr>
<td></td>
<td>• Works for IP and non-IP networks</td>
<td></td>
</tr>
<tr>
<td>SSL VPN</td>
<td>• Enables access control with finer granularity</td>
<td>• Implementations differ between vendors</td>
</tr>
<tr>
<td></td>
<td>• Uses a web browser as a client</td>
<td>• New, evolving technology</td>
</tr>
<tr>
<td></td>
<td>• Standardized</td>
<td>• Not all applications work</td>
</tr>
</tbody>
</table>
Appendix C

Wireless Security Technologies

Wireless Personal Area Networks (WPANs)

Bluetooth is a Wireless Personal Area Network (WPAN) technology intended primarily for cable replacement. It offers simple connectivity between a number of personal devices and corresponding peripherals, such as headsets, phones, printers, keyboards, and pointing devices. It also supports consumer electronics such as cameras and VCRs.

Current Bluetooth issues include Bluejacking (anonymous sending of unsolicited, potentially obscene messages to improperly configured devices) and Bluesnarfing (exploiting manufacturer flaws to obtain and manipulate data on a device). It is possible to ward off most threats with strict policies for device configuration and update procedures that ensure patching of flawed firmware. This highlights the need to implement a comprehensive mobile device management solution.

Wireless Local Area Networks (WLANs)

There are three acceptable ways to secure Wireless Local Area Networks (WLANs) today: WiFi Protected Access (WPA), virtual private network (VPN) with IP security (IPsec), and network access control. Another alternative is to leave wireless access points entirely open and unsecured, but place them outside the perimeter (firewall) of the network. This enables use by vendors and visitors who need wireless access, for example.

WPA

WPA provides acceptable security using either a pre-shared key (PSK) or in conjunction with the 802.1X protocol and Remote Authentication Dial-In User Service (RADIUS). For enterprises, the 802.1X protocol is advisable because PSK management does not scale easily or provide user-based authentication.

The advantages of this approach are that it involves the least infrastructure and is most efficient in bandwidth. The disadvantage is that all the Network Interface Cards (NICs) and access points (APs) must support WPA. Large implementations may therefore experience significant costs for upgrading and replacing equipment.

VPN

Wireless connectivity can be protected with a VPN. With this technique, all WiFi APs must be placed in a virtual local area network (VLAN) that terminates at a VPN concentrator. Users must authenticate to the VPN to access the network, which also ensures that the content is encrypted. The benefit of a VPN is that it is a proven technology that works with all NICs and APs. The disadvantage is that it adds about 30 percent of overhead onto the data being transmitted, which constrains air traffic in environments limited by capacity. In addition, the network must be configured to use VLANs and a VPN concentrator must be available.

Network Access Control

The 802.1X protocol provides a limited form of network access control—to gain access to a network, the user must successfully authenticate. However, no other controls limit user authorization. To address the need for refined access control, new products are appearing in the market. They are known as role based access controls (RBACs), network access controls, or simply wireless switches.
These appliances require the user to start a browser session before accessing the network. A switch redirects the browser to an authentication page and typically authenticates to a RADIUS server. In addition to simply allowing or rejecting access, they can constrain access based on any combination of time of day, user group, location (VLAN), target subnet, and target application. For example, employees in the finance department may be allowed to access the payroll system from their offices at any time. From the lobby, access to the payroll system could be restricted to office hours and access to email could be allowed at any time.

Beyond the virtually unlimited combination of access control rules, these products can offer enhanced services such as bandwidth throttling and over-the-air encryption. They are similar to a VPN. In some respects, they are a VPN superset because a VPN client operates between the client and the switch. Network access control is NIC/AP independent but requires dedicated equipment, which can be expensive. It is ideal in environments with highly diverse user groups for limiting access to the resources and applications that each group needs. Some of the main customer segments include educational institutions and airports. Universities have diverse needs for groups such as professors, administrators, students, visiting professors, and guests. Airports have diverse needs for venue operators, passengers, airlines, airport security, and baggage handling.

Table C–1 summarizes the WLAN technologies discussed, including their advantages and disadvantages.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
</table>
| WiFi Protected Access (WAP) | • Little additional infrastructure  
• Efficient bandwidth | • NICs and APs need to support WPA (adds cost to upgrade and replace equipment) |
| VPN (IPsec)                 | • Proven technology                             | • Adds 30% overhead                                |
|                             | • Works with all NICs and APs                   | • Can constrain air traffic                        |
| Network access control      | • NIC/AP independent                            | • Requires dedicated equipment (adds cost)         |
|                             | • Ideal for highly diverse sets of users       |                                                    |

Wireless Wide Area Networks (WWANs)

Today's Wireless Wide Area Networks (WWANs) include security provisions that are enforced by mobile terminals and base stations. Current examples of WWANs include Global System for Mobile Communications (GSM), General Packet Radio Service (GPRS), IS-95 Code Division Multiple Access (CDMA), IS-136 Time Division Multiple Access (TDMA), and Single Carrier Radio Transmission Technology (1xRTT). As the third generation of phone networks begins to roll out, enhancements to these mechanisms will further improve the authentication and privacy of wireless transmissions.

Although encryption algorithms provide an effective barrier to the vast majority of attackers, it is important to realize that they, like virtually all other encryption methods, are not uncrackable. Both the CDMA and GSM algorithms are reported to have been cracked. The value of the protection does not lie in providing a completely secure environment for sensitive transactions. Instead, it offers an obstacle so that monitoring and interception of random or bulk transmissions is simply not cost-effective or easy for a casual or unsophisticated attacker.
Appendix D

Types of Firewalls and Open Source Initiative (OSI) Layers of Operation

<table>
<thead>
<tr>
<th>Type</th>
<th>Layer of Operation (OSI Model)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packet Filters</td>
<td>Network</td>
</tr>
<tr>
<td>Circuit-Level Gateways</td>
<td>Session</td>
</tr>
<tr>
<td>Stateful Inspection Firewalls</td>
<td>Network, Transport, potentially others</td>
</tr>
<tr>
<td>Application Proxy Servers</td>
<td>Application</td>
</tr>
</tbody>
</table>

Packet Filters

Packet filtering is pervasive in today’s network environment, and implementations exist in routers, switches, and operating systems (OSs). Packet filters operate at the network layer and make decisions to allow or deny a particular network packet based on its content. Packet filters can be configured to allow or deny a packet based on the source or destination IP address; the User Datagram Protocol (UDP), Transmission Control Protocol (TCP), or Internet Control Message Protocol (ICMP) source or destination port; or the TCP acknowledgement bit. Packet filters are stateless, and they operate very efficiently due to the simplicity of their technique. However, they are vulnerable to spoofing (attacks based on falsified addresses and ports). In addition, they cannot defend against illogical packet sequences intended to disable or penetrate network hosts.

Circuit-Level Gateways

Circuit-level gateways establish sessions between trusted hosts and clients. Like proxies, they enable clients and servers to communicate without a direct connection. Many circuit-level gateways are based on the SOCKS protocol, which enables clients that have been properly modified to use a SOCKS gateway to access TCP applications without revealing their IP addresses. SOCKS works with virtually any TCP application, including web browsers and FTP clients. SOCKS gateways can act as simple firewalls by examining incoming and outgoing packets and determining whether to allow them based on configured rules.

Stateful Inspection Firewalls

Stateful inspection firewalls allow or deny network traffic based not only on the contents of individual network packets but also on the state of existing conversations. This is crucial for preventing attacks that present unexpected or spoofed packet sequences to network hosts in hopes of penetrating them or denying service to others. In order to determine whether a particular packet is part of a legitimate interaction, these firewalls build and use state tables with information from all seven layers of the Open Source Initiative (OSI) reference model. Stateful inspection firewalls are critical for protecting major networks.

Application Proxy Servers

Application proxy servers (proxies) are application-layer firewalls. Proxies provide security by breaking the direct connection between client and server, concealing network topology, and (in many cases) providing access control and communication security. Proxies add overhead by dividing each client-server connection into two connections, but they can also reduce network congestion by caching frequently
used web pages. Proxy server software can run on dedicated or shared general-purpose systems, or it can be prepackaged as part of a proxy appliance. Some proxies mediate web access only; others handle a wide variety of protocols.

*Forward proxies* are placed between client systems used to access the Internet and the Internet itself. Forward proxies can restrict Internet access, serving as one element of a layered defense against external attacks on internal systems. Forward proxies can be used to authenticate users and establish secure communication sessions with them. *Reverse proxies* are placed between Internet-facing applications and their users. Application users must communicate with the application through the proxy. Users may not be aware of this, since they use the application’s domain name (for example, [www.myapp.com](http://www.myapp.com)) as they would with direct, non-proxyed access. However, the Domain Name System (DNS) resolves the domain name to the IP address of the proxy rather than the application. Figure D–1 shows forward and reverse proxy configurations.

---

**Figure D–1**
Forward and Reverse Proxy Configurations

---

**Firewall Network Architectures**

There are three basic architectures of firewalls on networks: dual-homed host, screened host, and screened subnet. A *dual-homed host* (Figure D–2) has two NICs, each connected to a different network segment. The firewall controls traffic between the two networks. For example, in a very simple network, the firewall could allow selected outbound traffic from a subset of hosts and selected inbound traffic from the Internet to another group of hosts. Systems, like firewalls, that are properly secured against access from untrusted networks, such as the Internet, are called *bastion hosts*. Host security is discussed in the Trusted Infrastructure chapter.

A *screened host firewall* (Figure D–3) is protected by a packet-filtering router that sits between the firewall and an untrusted network. The router’s access control list (ACL) can be configured to allow traffic that meets specific source, destination, direction, port, and protocol criteria. Because the firewall receives only prescreened data, it can perform more detailed tests, such as stateful packet inspections, without adversely affecting network performance.
Although both dual-homed host and screened host firewalls provide basic security, most organizations require additional protection from attacks that originate on the Internet. The screened subnet (Figure D–4) network architecture includes a screened host firewall. It also segregates internal systems from systems attempting to access them from the Internet or another untrusted network. The Internet-accessible systems, configured as bastion hosts, are placed in a buffer zone or demilitarized zone (DMZ) directly behind the screened host firewall. The internal systems are segregated from the Internet-accessible systems in their own subnet, which is separated from the DMZ by a router, a firewall, or both. In this way, a minimum of three devices must be compromised before an external attacker can reach an internal system.
Appendix E

Authentication, Authorization, and Auditing (AAA) Servers

AAA (Triple-A) servers authenticate network users, authorize them to use particular network resources, and audit their network usage. AAA servers provide a central control point for external network access, and they work with various types of network access servers that interact with users and collect their credentials. All AAA servers must support a client-server security model in which:

- The network access server collects users’ credentials and requests authentication from the AAA server.
- The AAA server returns authorization information and other parameters.
- The network access server sets up a connection and writes an audit record.

AAA protocols must support multiple authentication methods, including user name and password, and multiple types of token authentication. They must also be extensible to accommodate future security requirements. There are three major AAA protocols today: RADIUS, Terminal Access Controller Access Control System+ (TACACS+), and DIAMETER (a play on the RADIUS acronym).

RADIUS

RADIUS, the most pervasive protocol, provides straightforward, efficient, and extensible services for authenticating individuals using a variety of credentials. It is available in a variety of implementations; however, it has no support for group membership, password management, account expiration, or event monitoring. Secondary authentication servers must be added to perform these functions in RADIUS environments. RADIUS uses User Datagram Protocol (UDP), which does not provide guaranteed delivery of messages between the network access server and the AAA server. It also does not, in its standard form, provide for confidentiality of client-server communication.

TACACS+

TACACS+ uses encrypted TCP packets for secure and reliable communication between clients and the AAA server, and it also logs system events such as access privilege changes. TACACS+ supports a wide range of security features compared to RADIUS, including group membership and privileges. TACACS+ can specify packet-filtering rules and access control lists (ACLs) for each session. However, TACACS+ is primarily a Cisco Systems protocol, and TACACS+ clients are principally Cisco appliances. In addition, its enhanced feature set and use of TCP give it greater network traffic overhead than RADIUS.

DIAMETER

DIAMETER is designed to overcome the limitations of RADIUS. It operates in a peer-to-peer mode; therefore, AAA servers can initiate requests themselves and handle transmission errors. It is also based on UDP, with enhancements for more reliable transport. Its other enhancements include support for roaming, cross-domain and brokered authentication, additional authenticable protocols, and enhanced security—including confidentiality and protection against replay attacks.
Glossary of Terms and Acronyms

The following glossary includes brief explanations for terms and acronyms used within this handbook. For additional definitions, please refer to http://searchsecurity.techtarget.com/glossary.

Numeric Terms

802.1Q is an IEEE standard for Virtual Bridged Local Area Networks. It specifies a general method for the operation of MAC bridges that support the construction of virtual LANs. For more information, see http://standards.ieee.org.

802.1X is an IEEE standard for port-based network access control. Its goal is to provide a means of authenticating and authorizing devices attached to a LAN port. For more information, see http://standards.ieee.org.

A

AAA or Triple-A (authentication, authorization, and auditing) refers to a framework for intelligently controlling access to computer resources, enforcing policies, auditing usage, and providing the information necessary to bill for services. These combined processes are considered important for effective network management and security.

AC (Active Countermeasures) refers to the HP Active Countermeasures service and technology. It is a distributed scanning tool that provides vulnerability analysis based on advisories from major security organizations. The tool scans the network for vulnerable machines and automatically deploys policy-driven mitigation techniques.

ACL (access control list) is a table that tells a computer operating system which access rights each user has to a particular system object, such as a file directory or an individual file.

AH (Authentication Header) is a protocol used with IPsec that provides authentication and data integrity services for transferred packets, but not encryption. It attempts to protect all fields of an IP datagram.

ANA (Adaptive Network Architecture) refers to the HP Adaptive Network Architecture service and technology. It is a network model that is composed of networking compartments, a virtual backbone that links the compartments, and a centralized policy management tool. The compartments are defined globally based on shared business requirements or characteristics, such as sales, suppliers, business applications, or call centers.

AP (access point) is a point of interconnection of users to other users on a network for transmitting and receiving data.

access control list See ACL.

access point See AP.

Active Countermeasures See AC.

Adaptive Enterprise is an HP strategy and process that helps end users prioritize their business needs and build upon their existing IT infrastructure to become more adaptive. The four main goals of the strategy are simplification, standardization, modularity, and integration.

Adaptive Network Architecture See ANA.
application proxy server is an application-layer firewall that provides security by breaking the direct connection between client and server, concealing network topology, and (in many cases) providing access control and communication security. Proxies add overhead by dividing each client-server connection into two connections, but they can also reduce network congestion by caching frequently used web pages. Proxy server software can run on dedicated or shared general-purpose systems, or it can be prepackaged as part of a proxy appliance. Some proxies mediate web access only; others handle a wide variety of protocols.

asymmetric keys are a pair of cryptographic keys that work together to encrypt and decrypt information. Asymmetric cryptography is also known as public-key cryptography.

attestation is the process of assuring the accuracy of information with reliable proof. In terms of identity management, attestation is the ability to determine who had access to which resources and in what timeframe. Attestation is also related to determining integrity within trusted platforms.

auditing is the process of logging, tracking, gathering, and analyzing activity to ensure regulatory and policy compliance, security from vulnerabilities, and accurate recordkeeping. Examples include logging all system administrator activity related to storage devices, analyzing audit logs within an IDS, and tracking the authorization, provisioning, and privacy components of an identity management system.

authentication is the process of confirming the correctness of a claimed identity. It can apply to an individual or a device such as a server. Passwords are commonly used to authenticate individuals. A digital certificate can be used to authenticate devices. Authentication precedes authorization.

authentication, authorization, and auditing See AAA.

Authentication Header See AH.

authorization is the process of granting approval, permission, or empowerment for an individual, device, or computer process that requests access to specific information, services, or functions. It is granted after authentication of the requestor’s identity.

availability ensures that the business purpose of a system is met and that systems and resources are accessible to those who are authorized to use them. See also CIA.

B

BIA (business impact analysis) is a component of a business continuity plan. It includes the examination of assets to identify vulnerabilities and a planning component to develop mitigation strategies for minimizing the potential risks from vulnerabilities.

BS 7799 See ISO 17799.

Basel II Accord is a framework that aims to improve the consistency of capital regulations internationally, make regulatory capital more risk sensitive, and promote enhanced risk-management practices among large, internationally active banking organizations. For more information, see www.federalreserve.gov/generalinfo/basel2.

bastion hosts are computer systems that are exposed to attack on the public side of a DMZ. Used as a security measure, bastion hosts are hardened to defend against attacks aimed at the inside network, and all unnecessary services, protocols, programs, and network ports are disabled or removed. Bastion hosts can include firewall gateways, web servers, FTP servers, name servers, mail hubs, and victim hosts (sacrificial lambs). See also screened-host firewall.
Bell-LaPadula is an access control model that mirrors the classification system used by most governments to label sensitive documents. It imposes a hierarchy of subjects and objects to decide whether a given subject is allowed to perform a certain action on a given object. The Bell-LaPadula model is concerned with the confidentiality of data.

Biba is a data integrity model that is identical to the Bell-LaPadula model, except that it deals with the reliability, consistency, and correctness of data.

Biometrics are technologies that facilitate the automated recognition of living persons based on behavioral or physical characteristics. Examples of characteristics include fingerprints, eye retinas and irises, voice patterns, and facial patterns. Biometrics are often used for authentication.

Bluejacking is the anonymous sending of unsolicited messages to improperly configured Bluetooth devices.

Bluesnarfing is the act of exploiting manufacturer flaws of a Bluetooth device to obtain and manipulate data.

Bluetooth is a WPAN technology intended primarily for cable replacement. It is commonly found on mobile devices such as PDAs, notebook computers, and cellular phones and used to connect to Bluetooth-enabled devices such as keyboards and headsets.

Business continuity describes the processes and procedures for ensuring that essential functions can continue during and after a disaster or crisis. Some best-practices legislation and frameworks, such as the Basel II Accord, require business continuity planning, which involves IT security and governance. See also Business Continuity Institute and DRI International.

Business Continuity Institute promotes standards for the provision and maintenance of business continuity planning and services. For more information, see www.thebci.org.

Business impact analysis See BIA.

C

CA (certification authority) is a trusted third party that authenticates users and issues digital certificates for public-key cryptography. In addition to establishing trust in the binding between a user’s public key and other security-related information in a digital certificate, the CA digitally signs the certificate information using its private key.

CDPD (Cellular Digital Packet Data) is a wireless transmission technology that uses unused cellular channels in the 800MHz to 900MHz range to support access to IP and ISO Connectionless Network Protocol (CLNP) networks.

CERT/CC is a computer emergency response team that works to identify and eliminate Internet threats and attacks. For more information, see www.cert.org.

CIA (confidentiality, integrity, and availability) refers to the triad of core characteristics that IT security exists to ensure.

CIAC (Computer Incident Advisory Capability) is run by the U.S. Department of Energy community for notification of computer security vulnerabilities and recommended actions. For more information, see www.ciac.org.

CISSPs (Certified Information Systems Security Professionals) have passed an exam that ensures that they have mastered a standardized body of knowledge in ten areas of system security. It is a vendor-neutral certification governed by the International Information Systems Security Certification Consortium (ISC²).
COBIT® (Control Objectives for Information and Related Technology) is a broad control framework for IT developed by the Information Systems Audit and Control Foundation (www.isaca.org) and the IT Governance Institute (www.itgi.org). COBIT divides IT into 34 process areas within four domains. It allows management to audit and evaluate how well IT processes align with business.

COPPA (Children’s Online Privacy Protection Act) applies to the online collection of personal information obtained from children under 13. The rules define what a web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent, and the responsibilities an operator has to protect children’s privacy and safety online. For more information, see www.coppa.org.

COSO (Committee of Sponsoring Organizations of the Treadway Commission) defines internal control processes. It is designed to provide reasonable assurance regarding objectives in the effectiveness and efficiency of operations, the reliability of financial reporting, and compliance with applicable laws and regulations. It requires a formal risk assessment to evaluate the internal and external factors that impact an organization’s performance. For more information, see www.coso.org.

CVE (Common Vulnerabilities and Exposures) is a list or dictionary that provides common names for publicly known information security vulnerabilities and exposures. For more information, see www.cve.mitre.org.

Canadian Privacy Act extends the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information. For more information, see http://canada.justice.gc.ca/en/ps/atip/.

Cellular Digital Packet Data See CDPD.

certificate See digital certificate.

certification authority See CA.

Certified Information Systems Security Professionals See CISSPs.

Children’s Online Privacy Protection Act See COPPA.

circuit-level gateways establish sessions between trusted hosts and clients. Like proxies, they enable clients and servers to communicate without a direct connection. This firewall approach validates connections before allowing data to be exchanged and monitors TCP or UDP sessions. Once a session is established, it leaves the port open to allow all other packets belonging to that session to pass.

Clark-Wilson is a proxy-based integrity model designed for the commercial environment and focused toward separation of powers or authorizations. Its goal is to prevent authorized users from making unauthorized changes to information.

cleartext is information in readable, unencrypted form. It is also known as plaintext.

Committee of Sponsoring Organizations of the Treadway Commission See COSO.

Common Vulnerabilities and Exposures See CVE.

compartmentalization divides networks into compartments or subnets to control security and other operational risks, facilitate standardization, establish least privilege access, and achieve a degree of redundancy. Many organizations use the structure of their business operations as an initial guide to compartmentalization.
Computer Incident Advisory Capability  See CIAC.

confidentiality  ensures that information is disclosed only to those who are authorized to view it. See also CIA.

confidentiality, integrity, and availability  See CIA.

Control Objectives for Information and Related Technology  See COBIT.

covert channels  are the means for communicating information between two parties in secret using normal system operations. An example is sending and receiving information between machines without alerting firewalls or IDSs on the network, using ports that the firewalls permit.

credentials  provide identification for gaining access to local and network resources. Examples of credentials include user names and passwords, smart cards, and digital certificates.

D

DAS  (Direct Attached Storage) is a storage device that is connected directly to a single system, similar to the disk within a PC.

DCID  (Director of Central Intelligence Directive) is a directive issued by the Director of Central Intelligence (DCI) that outlines general policies and procedures to be followed by intelligence agencies and organizations under DCI authority.

DCOM  (Distributed-Component Object Model) is a Microsoft technology that allows Component Object Model (COM) components to communicate over network boundaries. It is being phased out in favor of Microsoft’s .NET technology.

DDoS  (Distributed Denial of Service) is a DoS attack mounted by a collection of machines that have often been compromised through malware. The most common delivery methods are distributing e-mail attachments and exploiting target systems to deposit the DDoS code.

DHCP  (Dynamic Host Configuration Protocol) is a network protocol for automatically assigning IP addresses to devices on a TCP/IP network. The device retains the IP address for the current session and releases the IP address when it disconnects.

DMZ  (demilitarized zone) is a carefully isolated compartment in a network. It shields an organization’s internal network from public networks and prevents unauthorized access to the internal network and data by outside users.

DNS  (Domain Name System) is the system that translates Internet domain names into IP addresses.

DoS  (Denial of Service) is an attack that stops authorized users from accessing a system resource or delays system operations and functions.

DRI International  administers educational and certification programs for business continuity planning and management. For more information, see www.drii.org.

DRM  (digital rights management) consists of technologies that prevent the unauthorized use of a file, such as music or video content, to protect the rights of the owner.

data partitioning  is a method of improving security by distributing data across multiple locations.
**datagrams** are IP message units or blocks of data that the Internet transports. Datagrams are also known as packets.

**demilitarized zone** See DMZ.

**Denial of Service** See DoS.

**DIAMETER** is an authentication, authorization, and auditing (AAA) protocol that provides an interoperability framework for network access or IP mobility. For more information, see www.diameter.org.

**Diffie-Hellman** is a key agreement protocol that allows two parties to exchange a symmetric key, which can be used for encryption.

digital certificate is an electronic file used in **public key cryptography** that binds information about its subject with the subject’s public key. It is used for **authentication** of individuals, service, and devices. It is also known as a **PKI certificate** and an **X.509 digital certificate**.

digital identity is an individual’s profile, identifier, authentication, and authorization data.

digital rights management See DRM.

**Direct Attached Storage** See DAS.

**Director of Central Intelligence Directive** See DCID.

**Distributed-Component Object Model** See DCOM.

**Distributed Denial of Service** See DDoS.

**Domain Name System** See DNS.

dual-homed host firewall has two network interfaces, each connected to a different network segment. The firewall controls traffic between the two networks. For example, the firewall could allow selected outbound traffic from a subset of hosts and selected inbound traffic from the Internet to another group of hosts. Systems that are properly secured against access from untrusted networks, such as the Internet, are called **bastion hosts**.

**Dynamic Host Configuration Protocol** See DHCP.

dynamic proliferation causes subjects and objects to change state too quickly to cost-effectively maintain a **TCB** perimeter.

**E**

**ERP** (enterprise resource planning) employs technology solutions in large companies or other organizations to manage resources. Resources can include customers, supplies, and business functions such as accounting.

**ESP** (Encapsulating Security Payload) is an **IPsec** protocol that provides confidentiality (encryption) and an anti-replay service. It should be used with authentication, either with the optional ESP authentication field (authenticated ESP) or nested in an **AH** message. Authenticated ESP provides data origin authentication and connectionless integrity. When used in tunnel mode, ESP also provides limited traffic flow confidentiality.
Encapsulating Security Payload See ESP.

encryption is the cryptographic transformation of data (called cleartext) into a form (called cipher text) that conceals the data’s original meaning to prevent it from being known or used.

enterprise resource planning See ERP.

EU Directive on Data Protection is a European Union (EU) law designed to enable data movement while protecting privacy. It includes standards for collection, storage, use, and disclosure of personal data. The directive applies to European organizations as well as foreign organizations that process personal data within the EU. The directive also includes guidelines to ensure that data is only transferred outside the EU when adequate protection is in place.

extranet is a public-private web site or portal specifically designed for selected workers and external trusted partners to conduct business and access a portion of an organization’s internal business data.

FedCIRC See US-CERT.

firewall is a logical or physical discontinuity in a network to prevent unauthorized access to data or resources. Firewalls permit or deny packets to be sent to their destinations based on filtering rules.

forward proxies are servers that accept client (web browser) requests, forward them to the Internet, and send the responses back to the requesting client. They are most often used to give an internal user access to the Internet.

GLB See Gramm-Leach-Bliley Act.

GPL (GNU Public License) provides for free access to software published under its terms. Users are allowed to copy, modify, and redistribute GPL software. Derivative works must retain the GPL. For more information, see www.gnu.org.

GPRS (General Packet Radio Service) is a packet-based wireless communication protocol based on GSM (Global System for Mobile) technology. It provides Internet connectivity for mobile devices.

gap analysis is a governance mechanism that highlights the differences between the current state of an objective and the desired future state to identify areas that require attention.

General Packet Radio Service See GPRS.

GNU Public License See GPL.

governance is the controls and policies that translate high-level business objectives, operational risks, and regulatory needs into the directives, objectives, and policies that drive security mechanisms. Governance is often classified as corporate governance, security governance, and IT governance.

Gramm-Leach-Bliley Act (GLB) is a U.S. law that includes provisions to protect consumers’ personal financial information held by financial institutions. For more information, see www.banking.senate.gov/conf./

HIPAA (Health Insurance Portability and Accountability Act) aims to improve portability and continuity of health insurance coverage in the U.S. HIPAA defines rules for the security and privacy of individually identifiable health information. For more information, see www.hipaa.org.
**HMAC** (hash message authentication code) is a type of message authentication code that uses a cryptographic hash function in combination with a secret key.

**hash** is a mathematical algorithm that creates a message digest, which is a short, fixed-length digital representation of a longer, variable-length message. Hash functions are used to detect message tampering.

**hash message authentication code** See **HMAC**.

**Health Insurance Portability and Accountability Act** See **HIPAA**.

**honeypots** are unprotected hosts or other resources that attract and log probes and attacks. They do not offer direct protection to a network. Honeypots can be used to lure attackers and analyze system weaknesses.

**IAS** (Internet Authentication Service) is the Microsoft implementation of a **RADIUS** server. It enables centralized management of user authentication, authorization, and auditing.

**IBE** (Identifier Based Encryption) is an encryption and decryption technology based on a private and a public key. The encryption key is typically a bit string that identifies the intended decrypting party by a means, and to levels of detail and uniqueness, that are chosen by the encrypting party.

**ICMP** (Internet Control Message Protocol) reports errors and relays messages between hosts and Internet gateways during **IP datagram** processing. The **PING** command is an example of ICMP status reporting.

**IDS** (intrusion detection system) gathers and analyzes information from various areas within a computer or a network to identify security breaches. It monitors activity patterns, configurations, policy violations and other information to detect intrusions (attacks from outside the organization) and misuse (attacks from within the organization). **IDSs** may be host based or network based. Host-based **IDSs** reside on servers and analyze audit logs and other indicators of system activity. Network-based **IDSs** use dedicated hosts that intercept and analyze network traffic. **IDSs** detect intrusions and other exploits such as privilege abuse by using predefined rules, predefined attack signatures, or observed deviations from normal activity (statistical anomalies).

**IETF** (Internet Engineering Task Force) is a large and open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. For more information, see **www.ietf.org**.

**IKE** (Internet Key Exchange) is an **IPsec** protocol used before the **ESP** or **AH** protocol exchanges to select encryption and/or authentication services. IKE also manages distributing and updating the symmetric (shared) encryption keys used by the **ESP** and **AH** protocols. IKE can also use the **Diffie-Hellman** method, which enables exchange of cryptographic keys between two parties in a manner that cannot be compromised by an attacker and does not depend on previously shared keys.

**IPC** (interprocess communication) is a set of interfaces that facilitate communication between multiple processes.

**IPS** (intrusion prevention system) is similar to an **IDS** except that in addition to detecting attacks, an **IPS** can also take action to stop or block suspicious activity. **IPSs** may be host or network based. **IPSs** may respond to an attack by dropping suspicious data packets, terminating suspicious sessions, denying user access to resources, reporting activity to other hosts that may also be vulnerable, or updating their own configurations to better address specific attacks. **IPSs** can integrate with **firewalls**, so that when an **IPS** detects a source of hostile traffic, the firewall works to block it.
**IPsec** (IP security) is a standard security protocol defined by the IETF. It provides network-level access control, connectionless integrity, data origin authentication, and data confidentiality services. It uses three protocols: AH, ESP, and IKE. IPsec is used for VPN implementations.

**IPT** (IP telephony) are technologies that use IP connections to exchange voice, fax, and other forms of information that have traditionally traveled over standard telephone lines. Voice over IP (VoIP) is a standardization of IPT.

**ISACs** (Information Sharing and Analysis Centers) were created by Presidential Directive 63 to share important information about vulnerabilities, threats, intrusions, and anomalies within and between industry sectors and the National Infrastructure Protection Center (NIPC). For more information, see the ISAC Council at www.isaccouncil.org.

**iSCSI** (Internet SCSI) offers storage networking over IP networks, but it is not yet in widespread use. iSCSI is an important addition to SAN technology because it enables a SAN to be deployed in a LAN, WAN, or MAN (local-, wide-, or metropolitan-area network).

**ISO** (International Organization for Standardization) is a network of the national standards institutes of 150 countries that develops a wide range of standards that serve as the framework for compatible technology worldwide. For more information, see www.iso.org.

**ISO 17799** is the best practices section of the original BS 7799, which contained two parts: BS 7799 Part 1 (best practices) and BS 7799 Part 2 (security management systems). ISO 17799 recommends best practices for the treatment of information assets using the common characteristics of confidentiality, integrity, and availability or CIA.

**ISV** (independent software vendor) develops and sells software products for one or more operating system platforms.

**ITIL** (IT Infrastructure Library) is a set of guides and best practices for IT service management set forth by the Office of Government Commerce (OGC) in the United Kingdom. HP adopted the ITIL standard in 1996.

**Identifier Based Encryption** See **IBE**.

**identity** is the set of characteristics and data that distinguish an individual or entity.

**identity management** is the set of processes, tools, and social contracts surrounding the creation, maintenance, and use of digital identities for people, systems, and services. It enables secure access to a set of systems and applications. Identity management has strong links to security, trust, and privacy management. It also delivers components of risk management.

**independent software vendor** See **ISV**.

**Information Sharing and Analysis Centers** See **ISACS**.

**integrity** is protecting data or information from corruption or unauthorized changes.

**integrity-checking system** maintains a database or master list of security attributes in a safe location. It checks files and directories against the list and flags any discrepancies or errors.

**International Organization for Standardization** See **ISO**.

**Internet Authentication Service** See **IAS**.
Internet Control Message Protocol See ICMP.

Internet Engineering Task Force See IETF.

Internet Key Exchange See IKE.

Internet SCSI See iSCSI.

interprocess communication See IPC.

intrusion detection system See IDS.

intrusion prevention system See IPS.

IP security See IPsec.

IP telephony See IPT.

IT Governance Institute assists enterprise leaders in their responsibility to make IT successful in supporting the enterprise’s mission and goals. It offers best practices for IT governance and its alignment with security governance. For more information, see www.itgi.org.

IT Infrastructure Library See ITIL.

J K L

J2EE (Java 2 Enterprise Edition) is a Java application development platform for large-scale computing.

JCA (J2EE Connector Architecture) provides a standard architecture for integrating heterogeneous enterprise information systems.

J2EE Connector Architecture See JCA.

Java 2 Enterprise Edition See J2EE.

KPI (Key Performance Indicator) is a measurable variable that an organization identifies is critical to meeting its objectives and goals.

Key Performance Indicator See KPI.

L2F (Layer 2 Forwarding) is a tunneling protocol developed by Cisco Systems that supports VPNs.

L2TP (Layer 2 Tunneling Protocol) is an IETF standard for connecting VPNs. It is based on Cisco System’s L2F protocol and Microsoft’s PPTP technologies.

LDAP (Lightweight Directory Access Protocol) is a protocol to locate organizations, individuals, and other resources such as files and devices in an Internet or intranet directory.

LSASS (Local Security Authority Subsystem Service) is a Microsoft Windows process that verifies a user login.

LUN (Logical Unit Number) is the standard protocol for accessing disk drives and disk arrays in a SCSI system. It addresses a segment of storage allocated to a specific application or server using a unique number.
**LUN masking** enables the network manager or administrator to limit the visibility of servers or departments to a specific LUN to help ensure security.

**Layer 2 Forwarding** See L2F.

**Layer 2 Tunneling Protocol** See L2TP.

**least privilege access** is the principle of granting users or applications the minimum amount of permissions necessary to perform their intended function.

**Liberty Alliance** is an open body working to address the technical, business, and policy challenges surrounding identity and web services. For more information, see www.projectliberty.org.

**Lightweight Directory Access Protocol** See LDAP.

**Local Security Authority Subsystem Service** See LSASS.

**Logical Unit Number** See LUN.

**M**

**MAC** (Mandatory Access Control) is a security mechanism that assigns a security level to both information and users. It ensures that users access only the data at the security level for which they are authorized.

**MSCAPI** (Microsoft Cryptographic API) is a cryptographic protocol.

**man-in-the-middle** is a form of trust exploitation attack in which the attacker becomes an intermediary in a communication session between two nodes in order to capture or alter information.

**Mandatory Access Control** See MAC.

**Microsoft Cryptographic API** See MSCAPI.

**migratable key** is a cryptographic key tied to a TPM that can be moved from the originating trusted platform to another system but only under the tight control of the owner of that system. It is used for device authentication. See also unmigratable key.

**mitigation** involves actions to prevent or reduce risks or adverse impacts.

**multi-level security** is a need-to-know or safe-to-know structure that defines who can know what. Multi-level security measures are designed to reduce unauthorized access to sensitive data.

**N**

**NAS** (Network Attached Storage) is a RAID (disk), tape, or other mass storage system that has an integral network connection such as Ethernet or FibreChannel and is generally used to offload file storage tasks from application servers.

**NAT** (network address translation) is a security technique that translates an IP address used within one network to a different IP address from another network. It is commonly found in routers and firewalls and used to protect an organization’s internal IP addresses.

**NIC** (network interface card) is an adapter or card that provides a computer with a network connection.
nPARs (node partitions) enable configuration of a single server complex as one large system or as multiple smaller systems. These multi-operating system hard partitions are designed to provide for complete isolation. See also vPARs.

NSA (National Security Agency) is a cryptologic organization that coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. For more information, see www.nsa.gov.

NSP (network security processor) is a device that handles cryptographic functions. It is designed to offload processor-intensive cryptographic functions from a general-purpose server.

National Security Agency See NSA.

network address translation See NAT.

Network Attached Storage See NAS.

network interface card See NIC.

network security processor See NSP.

node partitions See nPARs.

non-repudiation guarantees that a transaction between two parties either did or did not occur. It eliminates or reduces claims that parties have not received a message and that the message has not been modified.

O

OASIS (Organization for the Advancement of Structured Information Standards) is a nonprofit global consortium that drives the development, convergence, and adoption of e-business standards. For more information, see www.oasis-open.org.

OECD (Organization for Economic Co-operation and Development) is an international standards organization. It provides guidance in many areas, including privacy policies to describe collection, limitation, data quality, and purpose specification principles. It sets important standards for governmental privacy rules. For more information, see www.oecd.org.

OSI model (Open System Interconnect model) is a seven-layer reference model that describes how information is transmitted between two points in a telecommunications network. It is an ISO standard that promotes product and device interoperability. The seven layers (from 1 to 7) are physical, data-link, network, transport, session, presentation, and application.

Open System Interconnect model See OSI model.

Organization for Economic Co-operation and Development See OECD.

Organization for the Advancement of Structured Information Standards See OASIS.

P

PII (personally identifiable information) is information that can be used to identify a person, such as a name, mailing address, Social Security number, e-mail address, or telephone number.
PKI (public-key infrastructure) allows for more secure exchange of information over public networks such as the Internet and requires a trusted authority known as a CA to issue digital certificates. It makes use of public-key cryptography for encrypted transmission of information.

**PKI certificate** See digital certificate.

**PPTP** (Point-to-Point Tunneling Protocol) is a protocol developed by Microsoft and others that can create VPN connections using the Internet.

**PSK** (pre-shared key) is an ASCII string agreed upon by two systems for encryption or authentication.

**packet filter** is a type of firewall or router that inspects incoming and outgoing packets to determine whether or not to forward them based on a set of defined security policies.

**personally identifiable information** See PII.

**port redirection** is a form of trust exploitation attack in which an attacker compromises a target system to listen on a certain configured port and redirects all packets to a secondary destination.

**ping sweep** is a network scanning technique that sends ICMP echo requests (PING commands) to a range of IP addresses in an attempt to find hosts that can be probed for vulnerabilities.

**plaintext** See cleartext.

**Point-to-Point Tunneling Protocol** See PPTP.

**port scan** is a series of messages sent to specific port numbers on a computer in an attempt to find a means of compromising the computer through a vulnerable port.

**pre-shared key** See PSK.

**proactive security management** focuses on managing security functions in support of business and organizational goals and processes. It manages the protection of data, applications, systems, and networks, both proactively and reactively; supports changes to business and organizational models; responds to a changing-threat environment; and integrates with IT infrastructure management and operations.

**provisioning** is the systems and processes within identity management that handle administrative functions such as add, modify, delete, and other maintenance and monitoring tasks.

**proxies** See proxy server.

**proxy server** is an intermediate server that sits between a client (for example, a web browser) and a remote server. It acts as conduit between the actual remote server and the client. A proxy server is used to improve performance and filter requests.

**public-key certificate** See digital certificate.

**public-key cryptography** is an encryption system that uses a pair of corresponding keys for encryption and decryption of information. One key is freely distributed (the public key) and the other is kept secret (the private key). See also PKI.

**Public-Key Cryptography Standards** (PKCS) #11 is a set of standards for public-key cryptography, developed by RSA Laboratories in cooperation with an informal consortium. It defines a technology-independent programming interface, called Cryptoki, for cryptographic devices such as smart cards and PCMCIA cards.
public-key infrastructure See PKI.

**Q R**

**RACF** (Resource Access Control Facility) is an IBM security application that provides access control and auditing functionality for mainframe operating systems.

**RADIUS** (Remote Authentication Dial-In User Service) is an AAA client-server protocol and proposed IETF standard that uses a central server to authenticate users and authorize access to requested systems or services from a remote device.

**RBAC** (role based access control) is a mechanism to map users to their permitted authorizations (operation, object). It is an umbrella term that includes the definitions of roles and authorizations.

**RFID** (Radio Frequency Identification) is a technology that uses radio frequency (RF) transmissions to identify specially tagged items. The system consists of two basic components, the ID tag and the tag reader. RFID readers generate an electromagnetic field that interacts with ID tags. The tags contain an antenna and microchips encoded with data.

**RSA** (Rivest-Shamir-Adleman) is an algorithm for asymmetric cryptography, invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.

**RSBAC** (rule set based access control) is a Linux-based security framework that consists of kernel enhancements and patches to implement access control.

**Radio Frequency Identification** See RFID.

**Remote Authentication Dial-In User Service** See RADIUS.

**residual risk** is the remaining risk after a mitigation plan is applied to a threat.

**Resource Access Control Facility** See RACF.

**reverse proxies** are servers that act as a gateway to backend web servers. They handle incoming requests from web browsers (clients).

**Rivest-Shamir-Adleman** See RSA.

**role based access control** See RBAC.

**rule set based access control** See RSBAC.

**S**

**SAML** (Security Assertion Markup Language) is an OASIS specification that provides protocols and formats for exchanging authentication and authorization information.

**SAN** (Storage Area Network) is a high-speed network that is typically part of an overall network of computing resources for an enterprise, in which the software knows the characteristics of storage devices and the quantity and value of data stored in those devices.

**SANS** is a source for system administration, audit, and network security information. For more information, see [www.sans.org](http://www.sans.org).

**SEM** (Security Event Management) is the ability to manage security events across the entire IT infrastructure.
SNMP (Simple Network Management Protocol) is a standard defined by the IETF for handling network management information. It is normally found as an application on top of the UDP. SNMP traps log alarms and diagnostics that describe network performance.

SOAP (Simple Object Application Protocol) was developed by Microsoft and provides a way for applications to communicate with each other via the Internet regardless of operating system. SOAP uses HTTP and XML to accomplish this.

SPIs (Smart Plug-ins) are the preferred integration method for linking security devices and applications into HP OpenView.

SPML (Service Provisioning Markup Language) is an OASIS specification and XML framework that provides provisioning capabilities for facilitating the creation, modification, activation, suspension, enablement, and deletion of identity-related data in different identity repositories.

SSH (Secure Shell) is a UNIX command interface that allows administrators to securely access and perform administrative tasks on remote servers.

SSL (Secure Sockets Layer) is a protocol for secure information exchange over the Internet. SSL facilitates secure information exchange by using digital certificates and a variety of encryption techniques.

Safe Harbor framework is an agreement that provides legal protection and a framework allowing for the safe transfer of personal information from European Union countries to the U.S. To qualify, an organization can join a self-regulatory privacy program that adheres to the framework’s requirements. Alternatively, it can develop its own self-regulatory privacy policy that conforms to the Safe Harbor framework. For more information, see www.export.gov/safeharbor.

Sarbanes-Oxley is U.S. legislation that ensures internal controls or rules for governing the creation and documentation of corporate information in financial statements. For more information, see www.sarbanes-oxley.com.

screened host firewall is protected by a packet-filtering router that sits between the firewall and an untrusted network. The router’s ACL can be configured to allow traffic that meets specific source, destination, direction, port, and protocol criteria. Because the firewall receives only prescreened data, it can perform detailed tests, such as stateful packet inspections, without adversely affecting network performance.

screened subnet architecture includes a screened host firewall. It also segregates internal systems from systems attempting to access them from the Internet or another untrusted network. The internal systems are segregated from the Internet-accessible systems in their own subnet, which is separated from the DMZ by a router, a firewall, or both.

sealed storage is a mechanism of a TPM that prevents the release of secrets conditioned upon the presentation of a valid authorization value, the presence of a particular TPM, and/or the verification of a particular software state. It prevents inappropriate access to encrypted files and network resources that would otherwise be vulnerable to attacks.

Secure Shell See SSH.

Secure Sockets Layer See SSL.

security architecture is all of the technology, people, and processes required to implement the security governance objectives of a business and to align the objectives with the requirements of IT governance, due diligence, and legislative compliance.
Security Assertion Markup Language See SAML.

Security Event Management See SEM.

security incident is an event outside the standard operation of a service that might force an interruption in the confidentiality, integrity, or availability of an IT system.

security incident management is the processes, people, and technologies that manage the prevention, detection, alerts, logging, investigation, and resolution of actual or potential security incidents.

Service Provisioning Markup Language See SPML.

Simple Network Management Protocol See SNMP.

Simple Object Application Protocol See SOAP.

single sign-on (SSO) is the ability of a user to authenticate once to a single authentication authority, obtain a credential token, and use it to access protected resources without re-authentication.

smart card is a plastic card, usually about the size of a credit card, containing an embedded integrated circuit. Smart cards can be used for electronic identification, storing medical records, and making purchases, among other things.

Smart Plug-ins See SPIs.

sniffer is a software tool that monitors network traffic. It can also be used by an attacker to discover information being transmitted in IP packets.

SOCKS is a networking protocol for handling Internet traffic through a proxy server. It acts as a simple firewall by checking incoming and outgoing packets and authenticating and authorizing requests based on the requested destination or user.

spoofing is an attack based on falsified IP addresses and ports.

spyware is software that gathers information or tracks users’ activity without their knowledge or permission.

state machine is a system model using subjects and objects. Each subject (program, process) and object (file, memory range) is assumed to have states, which change over time (state transitions). A simple example of subjects and objects might be {man, boy, bat, ball}. Acceptable states might be {accelerating, decelerating, stationary}.

stateful inspection firewalls allow or deny network traffic based on the contents of individual network packets and the state of existing conversations. In order to determine whether a particular packet is part of a legitimate interaction, these firewalls build and use state tables with information from all seven layers of the OSI model.

Storage Area Network See SAN.

subnet is an abbreviation for subnetwork. It is an identifiably separate part of an organization’s network, such as all the machines at one geographic location, in one building, or on the same LAN. Subnets are used to configure multiple network connections between devices, and they can be connected to the Internet with a single shared network address.
**TACACS+** (Terminal Access Controller Access Control System +) is a AAA client-server protocol developed by Cisco Systems for remote access.

**TCB** (Trusted Computing Base) is the security perimeter or the set of subjects and objects over which the security administrator has control and assurance.

**TCG** (Trusted Computing Group) develops and promotes open specifications for trusted infrastructures. Computing industry vendors use these specifications in products that protect and strengthen the computing platform against software-based attacks. For more information, see [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org).

**TCPA** (Trusted Computing Platform Alliance) addresses the issues of Trusted Computing Platforms and is the predecessor organization of the TCG. For more information, see [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org).

**TLS** (Transport Layer Security) is the successor to the SSL protocol for encrypted information exchange, as proposed by the IETF.

**TNC** (Trusted Network Connect) is a TCG working group that defines an open-solution architecture for network administrators to enforce security policies for endpoint host connections to their multi-vendor networks. For more information, see [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org).

**TPM** (Trusted Platform Module) is an integrated circuit that provides logical and physical protection for keys and secrets. For more information, see [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org).

**TTP** (Trusted Third Party) is an organization that participants in a transaction agree is trustworthy and that provides a service to the participants. A CA is an example of a TTP.

**Terminal Access Controller Access Control System +** See TACACS+.

**traffic analysis** is the analysis of communication patterns between network hosts.

**Transport Layer Security** See TLS.

**Triple-A** See AAA.

**Trojan horse** is a program that appears legitimate, but it performs some illicit activity when run. It may be used to locate password information, make the system more vulnerable to future entry, or destroy programs or data on a hard disk.

**troble ticket system** is a system that tracks and manages security or support incidents.

**Trusted Computing Base** See TCB.

**Trusted Computing Group** See TCG.

**Trusted Computing Platform Alliance** See TCPA.

**trusted infrastructure** is composed of hardware platforms, together with their operating environments and applications, that behave in an expected and predictable way for their intended purpose. Trusted infrastructures support the IT applications underlying critical business processes. It implements appropriate technologies to secure an organization’s end-to-end IT infrastructure.

**Trusted Network Connect** See TNC.
Trusted Platform Module  See TPM.

Trusted Third Party  See TTP.

U V

**UDP** (User Datagram Protocol) is a communications protocol used instead of TCP with IP. Unlike TCP, UDP does not acknowledge or guarantee delivery, and it does not provide sequencing of packets.

**US-CERT** (United States Computer Emergency Readiness Team) is a central information technology incident coordination and analysis facility of the civilian agencies and departments of the U.S. government, such as the Department of Homeland Security. The FedCIRC advisory and response team is now part of US-CERT. For more information, see www.us-cert.gov.

**United States Computer Emergency Readiness Team**  See US-CERT.

**unlawful disclosure** is the risk associated with the loss of privacy.

**unmigratable key** is a cryptographic key for TPM certification that is locked to the trusted platform from which it originates. It is used for device authentication. See also **migratable key**.

**User Datagram Protocol**  See UDP.

**VLAN** (virtual local area network) is a LAN that defines network membership on a logical basis rather than a physical basis. It can be used to resegment networks without rewiring them and to partition hosts and host traffic based on business and security requirements rather than physical location.

**vPARs** (virtual partitions) provide application and operating systems isolation executing on single-server nodes or within single-system hard partitions. Each virtual partition runs its own operating system image and can host its own applications, offering complete software isolation. See also **nPARs**.

**VPN** (Virtual Private Network) is a private network that utilizes parts of the public telecommunications network, such as the Internet. VPNs send encrypted data through the public network to ensure the security of transactions.

**VPNC** (Virtual Private Network Consortium) enables organizations to use the public Internet for secure communications. For more information, see www.vpnc.org.

**virtual local area network**  See VLAN.

**virtual partitions**  See vPARs.

**virtual private network**  See VPN.

**Virtual Private Network Consortium**  See VPNC.

**virus** is software used to infect a computer. After the virus code is written, it is buried within an existing program. Once that program is executed, the virus code is activated and attaches copies of itself to other programs in the system. Infected programs copy the virus to other programs.

**vulnerability scanning software** is a software utility that proactively identifies security vulnerabilities and risks.
W

**WINS** (Windows Internet Naming Service) manages assignment of workstation names and locations with IP addresses.

**WLAN** (Wireless LAN) is a network for mobile devices which can connect via a wireless RF connection. The *IEEE 802.11* standard specifies the technologies for wireless LANs.

**WPA** (WiFi Protected Access) provides security by encrypting data sent over radio waves from one wireless device to another wireless device and by controlling access to network resources through authentication protocols.

**WPAN** (Wireless Personal Area Network) is a wireless network that serves a single person or small workgroup. It typically has a limited range (less than 10m) and is used to transfer data between a laptop PC or PDA and a desktop PC, server, or peripheral device. See also Bluetooth.

**WS-** is a collection of web services protocol specifications developed by Microsoft.

**WS-Security** (Web Services Security) is an OASIS standard that enables additional protection of SOAP messages.

**war dialing** is using a software program to attempt to identify telephone numbers that connect to modems.

**war driving** is the process of locating wireless access points by driving around a city and then attempting to exploit them or use them for free.

**Web Services Security** See WS-S.

**WiFi Protected Access** See WPA.

**Windows Internet Naming Service** See WINS.

**Wireless LAN** See WLAN.

**Wireless Personal Area Network** See WPAN.

**wiretapping** is the eavesdropping on and recording of data transmissions.

**worm** is a destructive program that replicates itself throughout disk and memory, using up computer resources until the system becomes unusable.

X Y Z

**X.509 digital certificate** See digital certificate.

**XACML** (XML Access Control Markup Language) is an OASIS standard that provides an open, XML-based method for access control.

**XKMS** (XML Key Management Specification) is an open standard that defines a web services interface to a PKI. For more information, see www.xmltrustcenter.org.

**XML Access Control Markup Language** See XACML.

**XML Key Management Specification** See XKMS.