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

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.

Figure 4–4
Enterprise Network Trends

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</td>
<td>Requires careful design</td>
</tr>
<tr>
<td></td>
<td>Works with geographically dispersed systems</td>
<td>boundaries</td>
<td>Requires increased cost and complexity with increasing number of compart-</td>
</tr>
<tr>
<td></td>
<td>Facilitates layered defense and standardization; flexible and adaptable</td>
<td>Accepts changes in business structure and operations without requiring</td>
<td>ments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>changes to the physical network</td>
<td></td>
</tr>
<tr>
<td></td>
<td></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 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

---

Access security controls which users have access to systems and how they connect in a wired and wireless world. HP ProCurve provides:

- Standard 802.1X port-based access control for all HP ProCurve enterprise-class managed products.
- 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.
- 802.1X used with 802.11 wireless networks to ensure only authorized users are granted access to the enterprise network.
- 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.

Management security includes the protection of the network infrastructure itself and prevents unauthorized users from overriding other security provisions. HP ProCurve provides:
• 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

---

Connection requests to host not in the Working Set are placed on the Delay Queue and set on a periodic timer.

If the number of queued connection requests exceeds the high water mark, virus-like activity is indicated.

The length of the delay queue and the points at which virus-like activity is recognized can be configured to adjust the sensitivity of the detection mechanism.

Each connection request is processed by the Virus Throttle Filter Driver.

The Working Set contains a list of the most recently connected hosts. Connection requests to these hosts are not delayed.
**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](http://www.hp.com/go/security/strategy) for details and updates about HP partner information.
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.
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.
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](http://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 ProCurve Networking</td>
<td>Network Security</td>
<td><a href="http://www.hp.com/go/procurve">www.hp.com/go/procurve</a></td>
</tr>
<tr>
<td>HP Virus Throttle</td>
<td></td>
<td>Click Security</td>
</tr>
<tr>
<td>HP Adaptive Network Architecture</td>
<td></td>
<td><a href="http://www.hp.com/go/services">www.hp.com/go/services</a></td>
</tr>
<tr>
<td>HP Active Countermeasures Service</td>
<td></td>
<td>Contact HP</td>
</tr>
<tr>
<td>HP ProLiant Essentials Intelligent Networking Pack</td>
<td></td>
<td><a href="http://www.hp.com/go/proliant">www.hp.com/go/proliant</a></td>
</tr>
<tr>
<td>HP ProLiant ES/IIP/NCP</td>
<td></td>
<td>Click Management Software, HP Intelligent Networking Pack (under Monitor &amp; Alert)</td>
</tr>
<tr>
<td>HP ProtectTools</td>
<td>Host Security</td>
<td><a href="http://www.hp.com/go/security">www.hp.com/go/security</a></td>
</tr>
<tr>
<td>HP-UX 11i</td>
<td></td>
<td>Click HP ProtectTools for Microsoft Products (under Featured Products and Services)</td>
</tr>
<tr>
<td>Linux</td>
<td></td>
<td><a href="http://www.hp.com/go/Linux">www.hp.com/go/Linux</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/tru6unix">www.hp.com/go/tru6unix</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>HP Atalla Security Products</td>
<td></td>
<td><a href="http://www.hp.com/go/atalla">www.hp.com/go/atalla</a></td>
</tr>
<tr>
<td>HP Security Services</td>
<td>Trusted Infrastructure Services</td>
<td><a href="http://www.hp.com/go/security">www.hp.com/go/security</a></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click on Security Services (under Featured Products and Services)</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.)

