PART I

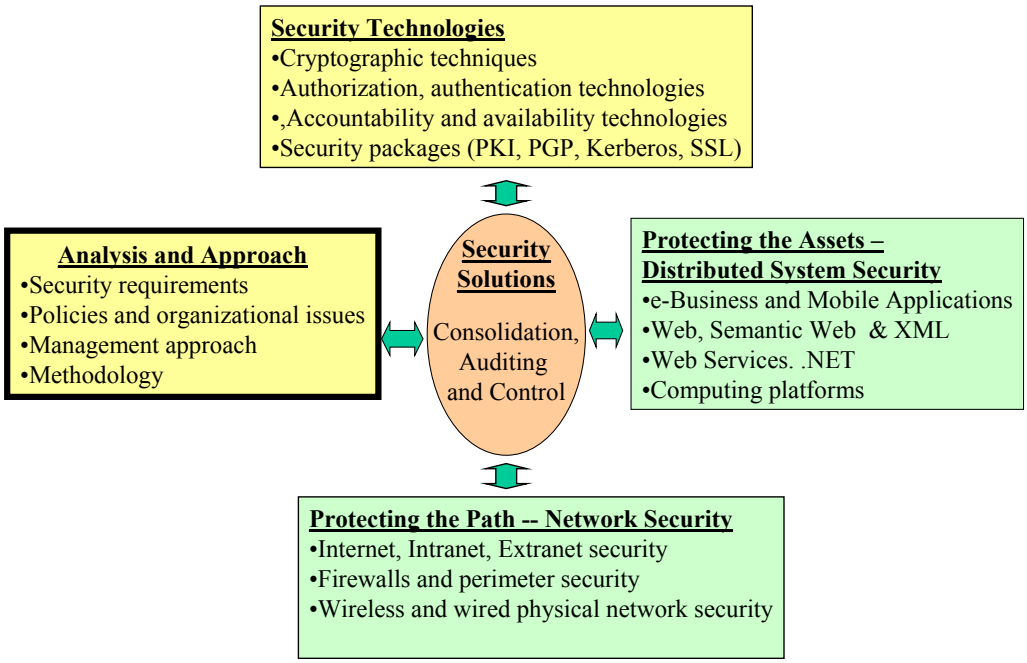
Analysis and Approach

This part of the book introduces security issues in modern digital environments and establishes an overall approach (box with dark borders in the framework shown below).

Chapter 1: Information Security and Auditing in Modern Environments – An Overview

Chapter 2: Security Management: Polices, Requirements, and Organizational Issues

Chapter 3: A Systematic Methodology: Linking People, Processes, and Technologies



1 Information Security in Modern Enterprises – An Overview

The World Trade Center Disaster and Recovery Planning

On September 11, 2001, two airplanes flew into the World Trade Center (WTC), killing more than 2000 people. All WTC offices were destroyed and many nearby buildings were badly damaged and immediately evacuated. Beyond the loss of human lives, major

services were disrupted[1]. Phone lines along the east cost of the United States were jammed due to the obvious increased phone activity. In addition, major telecommunication providers such as AT&T and Verizon lost major portions of services because their major switching centers and computer systems were located in areas near the WTC. This impacted several major clients, including Lufthansa Airlines which lost telephone services for its sales offices in downtown Manhattan. Lufthansa had chosen AT&T as its primary and Verizon as a backup provider. With both facilities impacted, Lufthansa was left without a telephone service for almost a week.

Many companies that relied on the Internet to conduct business were not severely impacted. In fact, the Internet became a viable alternate vehicle for communications in that disastrous week. In my own office in New Jersey that afternoon, we could not get the news from TVs (no TVs were available in the offices), so we all visited the news sites from CNN, FOX and others to understand what was going on. Internet telephony and email became the primary source of communicating with family and friends to let them know that we were OK.

Merrill Lynch had over 9,000 employees working at the WTC and the nearby World Financial Center. Most were unharmed and were relocated to other places of work quickly and successfully. Merrill resumed its business later in the same day and did not suffer as much as others. The main reason was that it had redundant telecommunications capabilities and a good disaster recovery plan. Merrill had rehearsed the plan four months earlier, so it was better prepared for a disaster than others. The plan included priorities for business activities, so that high priority activities could be brought online quicker. It also included detailed procedures for restoring critical applications with procedures that included necessary technologies, personnel, and facilities for a quick restoration in case of a disaster. Logistics were also in place for transportation of personnel and equipment, with provisions for housing and feeding employees for up to 8 weeks. This disaster recovery plan went into action within minutes after the incident and Merrill was operational later that day.

Source (abbreviated from): Laudon and Laudon, *Management Information Systems*, 8th Edition, Prentice Hall, 2003.

1.1 Introduction

We are living in an Internet-based digital age that is gradually affecting everyday life, restructuring business relationships and enabling new commerce activities, processes, and business models that were previously unimaginable. Use of the Internet for entertainment, online purchases, and conducting business grew dramatically in 1999 but slowed down considerably in 2001. Despite the slowdown in 2001, the digital environments continue to grow, and the volume as well as the value of Internet transactions continues to increase. According to an International Data Corp. (IDC) report

[1] I was in the area shortly afterwards and have not been able to forget it.

released in March 2002, the number of Internet users worldwide will double between 2001 and 2006, increasing from 500 million to 1 billion. Most of this growth will come from outside the United States.

This growth has brought about fundamental shifts in how business is carried out by enterprises, how enterprises do business with each other, how they interact with their customers, and in the mix and distribution channels of new products and services. In today's marketplace, across all industry segments, businesses as well as consumers are adopting a digital lifestyle with high reliance on information technologies. For example, enterprises around the world are increasingly leveraging information technologies to:

- Broaden their markets by extending their reach globally at minimal additional expense and enticing new prospects to become customers
- Enter new business areas through collaborations or expanded services made possible with Web-based interactions
- Increase employee productivity by providing easier access to corporate information and services
- Reduce costs through improved operations that integrate Web access and traditional IT systems
- Achieve operating efficiencies by reducing the number of people making routine decisions, by decreasing turnaround time, by managing reduced inventories, etc.
- Combine faster response times, continuous availability, and an ability to deal with complexity through the use of e-business applications to enable business opportunities that couldn't be made profitable in a manual implementation.

Despite the current economic slump, many companies are moving towards a digital enterprise model by using e-business for strategic reasons (see the sidebar "Why Move Towards Digital Enterprises?"). Some companies are very aggressively adopting the digital enterprise model. For example, ***"real-time enterprise models"*** are gaining popularity at the time of this writing. In the real-time enterprises, the interactions between business activities within an enterprise are conducted, monitored, and controlled electronically in real time. In addition, external communications with business partners are conducted through trading networks that support B2N (business to network) interactions. The Internet-based IT infrastructure becomes *the* primary source of company business in this model. Large corporations such as GE have adopted this model (see the sidebar "GE Becomes a Real-Time Enterprise"). It is also well known that most current and future military operations are performed through sophisticated information systems that range from real-time embedded systems to chat groups.

While our reliance on these technologies is increasing, so is the concern about the security and reliability of the technologies that are driving the modern digital environments. Imagine, for example, the impact of security attacks on real-time companies such as GE along with several other civilian and military operations that rely 80-90% on IT. This chapter takes a broad look at the issues and develops an overall solution approach that is followed as a roadmap.

Why Move Towards Digital Enterprises?

- **Economic reasons.** These are the main drivers, naturally. For example, labor costs traditionally keep going up and more staff is needed to market and support products. However, e-business lowers cost of labor due to the replacement of labor with Web-

based advertising and purchasing. In particular, Web-based advertising allows companies to reach a much wider customer base without expensive marketing personnel. In addition, online purchasing can provide 24/7 purchasing of goods without any sales personnel. For example, by using the Internet to interact with customers, Proctor and Gamble has cut its marketing research costs by 50 to 75 percent. Numerous companies such as General Electric, Cisco, Dell, Northwest Airlines (in fact, most airlines), and Amazon.com effectively use Web-based advertising and purchasing to reach more customers around the clock at more sites but with lower costs.

- **Possible improvements in business processes.** Significant improvements in procurement and order fulfillment are driving several companies to e-business. For example, IBM found that the time to fill orders dropped from 30 days to 1 day, and the contract negotiation time dropped from 6 months to 1 month, by using e-business. Survival is pushing many companies to move to e-business, because if they do not, they could be annihilated by the competition.
- **Reduction of transaction costs.** Business transaction cost is the cost incurred by a firm when it buys in the marketplace what it cannot make itself. Using markets is expensive because of costs such as locating and communicating with distant suppliers, negotiating contracts, monitoring contract compliance, etc. Over the years, firms like General Motors have attempted to minimize transaction costs by doing things themselves and buying many of their supplier companies – thus getting bigger [Williamson 1985]. e-Business with automated supply chains and e-markets reduces transaction costs dramatically. For example, HP developed an automated supply chain that reduced the time to build a PC to 48 hours. This eliminated the need for HP to keep PC inventories on hand.
- **Facilitate quick adaptation.** Businesses need to adapt quickly (e.g., enter new markets, redefine focus), reduce cycle time (e.g., set up a new large-scale business in 6 months), improve responsiveness, give better financial and operational flexibility, and improve utilization of resources. This is becoming increasingly possible with the Internet.
- **Significant reduction of paperwork.** For example, Staples has significantly reduced paperwork by using e-business. According to an August 26, 2002, *Wall Street Journal* advertisement, 3.3 million corporate end-users of Staples use real-time order information on over 80,000 items. The items are available at the Staples website (www.staples.com), which displays on-hand inventory instantly and handles customer orders.
- **New and improved organizational structures.** e-Business impacts organizational structures by changing the hierarchy of decision making and reducing the need for middle management and clerical support. Different levels of managers can interact directly through a corporate Intranet. In addition, firms can exist entirely or partially on the Web, leading to ***virtual enterprises.*** These enterprises tie suppliers to consumers and eliminate a complete organizational structure. For example, Corolla is a virtual flower shop that gets online orders for flowers from customers and routes the orders directly to the farmers. This "flower shop without any flowers" eliminates the need for a flower store where the farmers bring their flowers to be sold.
- **Reaching new customers**. Companies rely on e-business to expand services and reach new customers. For example, Dell Computers used e-business to reach customers directly and to deliver custom-built computers by adopting a "build-to-

order" model. This completely changed the dynamics of the PC industry and took big players such as IBM and Compaq by surprise.

- **Market Differentiation**. e-Business services provide market differentiation to many companies. For example, Amazon.com provided a market differentiation by offering around 1.5 million book titles while average bookstores offered about 50,000 book titles. Keep in mind, however, that these market differentiations can also quickly disappear.
- **Increased outsourcing options.** Outsourcing through the Internet (i.e., utilizing the Internet to move business services and functions outside the corporation) saves operational and support costs in installation, repair, shipping, and inventory management. Numerous ASPs (Application Service Providers) such as Corio host a complete set of business applications to facilitate partial or complete outsourcing of business information systems.
- **New business partnerships.** Business partnerships are being formed at the function level because competition has moved to the individual business functions (services) within a company instead of the overall company business. For example, if company A provides a better call center but company B builds better software quickly, then partnering with A for call centers and with B for software development makes better business sense.
- **Potential of eMarkets.** Electronic marketplaces and trading hubs (i.e., virtual internet "stores" offering products and/or services from many vendors) became popular to provide improved services for buyers. Examples exist in business-to-consumer (e.g., Amazon, MSN), consumer-to-consumer (e.g., eBay), and business-to-business (e.g., FastParts, COW) transactions. Interesting examples of emarkets can be found in the Telecom eMarkets such as Arbinet and Band-x. Although not fully realized, emarkets have a great deal of potential, especially if systems supporting business functions such as inventory, supply chain, network design, etc. are integrated with electronic markets.

Source: Umar, A., *e-Business and Distributed Systems Handbook: Overview Module*, NGE Solutions, May 2003. Available through Amazon.com.

GE Becomes a Real-Time Enterprise

General Electric (GE) is the world's largest diversified manufacturer, with $155 billion in revenue and 460,000 employees in 100 countries. Despite its size and old-economy businesses, *Internet Week* named GE its e-business company of 2000. GE started conducting purchasing and selling on the Internet in the mid 1990s with some early successes. For example, GE Plastic's distribution arm (Polymerland), began distributing technical documentation over the Web in 1994 and put its product catalog on the Web in 1995. In 1996, GE Lighting reduced its purchasing cycle from 14 to 7 days and also reduced its supply prices by 10 to 15 percent because of open bidding on the Internet. In 1997, seven other GE units began purchasing via the Internet.

Fast forward to November, 2002. Gary Reiner, current CIO of General Electric Co., uses

a large keyboard and a huge screen display panel that shows the real-time status of software applications critical to GE's day-to-day operations. The screen displays an array of green (indicates good), yellow (not as good as it could be) and red (trouble) icons that represent the status of GE's operations around the globe. For example, Reiner uses the main screen for GE's plastics operation, which flashes a series of green lines and a few yellow lines. If red bars appear on the screen, Reiner sends an email to the appropriate division manager asking for an immediate explanation. His goal is to monitor, once every 15 minutes, GE's mission-critical operations such as sales, daily order rates, inventory levels, and other important activities across the company's 13 different businesses around the globe. The icons of up-to-the-minute *business* performance across the company are checked regularly by *agents* that send test transactions to exercise various business operations such as an online purchase. These transactions typically take a few seconds to complete and trigger an automatic email or inquiry when the status is yellow or red. The main idea is to respond to changes and manage risks continuously instead of waiting for end-of-the-month or end-of-the-quarter reports.

GE estimates that its digitization efforts saved the company $1.6 billion in 2001. "We said we'd cut $10 billion in costs in five years, and we're already a third of the way there," Reiner says.

Sources:

- Dave Lindorff, "GE's Drive to Real-Time Measurement," *CIO Magazine*, November 11, 2002
- Umar, A., *e-Business and Distributed Systems Handbook: Overview Module*, NGE Solutions, May 2003. Available through Amazon.com.

1.2 Security Issues Unique to the Digital Age

Increased reliance of modern enterprises on applications and the IT infrastructure (networks, computing platforms, middleware services) to support these applications is creating new security and intrusion threats. In particular, the increased reliance on the Internet has introduced several security risks due to the almost unlimited supply of hackers, intruders, and eavesdroppers. For example, the 1998 annual report from the Computer Emergency Response Team (CERT) lists over 1300 reported security incidents on the Internet, affecting nearly 20,000 sites [CERT99]. The number of worms, viruses and distributed denial-of-access attacks is growing at a 120 percent rate, year after year, and is resulting in calls to let the private sector run the Internet [Cooper 2003].

1.2.1 The Vulnerabilities and Issues

Although security has been around for several years, modern digital environments in this post 9/11 (September 11, 2001) era create several vulnerabilities that are unique and different. Here are some examples.

- **Impact due to Size and Openness.** Large public networks, such as the Internet, are vulnerable, just because they are so large and virtually open to anyone that, when

abuses do occur, they can have an enormously widespread impact. For example, a virus delivered through emails over the Internet can infect hundreds of thousands of organizations within an hour.

- **Increased Virus Attacks and Assaults.** Many viruses are being introduced on an almost continuous basis. Almost every other week, we hear about yet another virus that could potentially disable our computer systems. As stated previously, the number of attacks is growing at a rate of 120 percent every year and in fact 9 out of the 13 root domain name servers that support the entire Internet went down due to distributed denial-of-service attacks in October 2002 [Cooper 2003]. Most of these viruses are examples of mobile code that operates covertly on computer systems. "Trojan horse" is an example. In addition, due to the 9/11 attack, issues of hacking versus assaults has been brought to the forefront. While hackers may be thought of as nuisance or "ankle biters," the assaults are intended to completely destroy your operation. Different measures are naturally needed for assaults versus hacking.
- **Increased Connectivity**. In the past, people connected to networks through dial-up lines on an as-needed basis. This situation has changed considerably. Most computers are at present permanently connected to the Internet through DSL, cable modem or other connections instead of through dial-ups. These computers have permanent IP addresses that can be accessed by the outsiders even when you are not doing anything. This "always on" connection increases the vulnerability to attacks by hackers. Basically, a fixed Internet address creates a fixed target for hackers.
- **Web-based Architecture Vulnerabilities**. As the Internet increasingly becomes part of the corporate network, the organization's information systems become vulnerable to actions from outsiders. As we will discuss extensively, the architecture of a Web-based application typically includes a Web client, a server, and corporate information systems linked to back-end databases. Each of these components are exposed to security challenges and vulnerabilities due to their connection to the Internet. Consider, for example, a database that has been used internally for several years but is now connected to the Internet. This new connection will expose the database to a much larger and more varied set of users (including hackers) than ever before.
- **Wireless and Mobility**. Increased use of wireless communications further increases the chances of eavesdropping and of compromising the integrity of information being transferred between sources and destinations. While it is possible to tap a wired connection also, wireless communications are easier to intercept by using simple antennas. For example, while the Wi-Fi (wireless local area networks) systems are quite popular, many vulnerabilities of Wi-Fi have been well documented (see, for example, *Communications of ACM*, May 2003, special issue on wireless security).
- **Web and Web Services**. Increased reliance on the Web creates several new vulnerabilities. For example, websites are under constant attacks from hackers for denial of service. Web Services (WS), the foundation of Microsoft's .NET, also creates very unique security challenges and risks. For example, WS allows numerous service providers to advertise and provide services by using a broker model. It is not exactly clear how to deal with security issues in such models.
- **Growing Middleware Stack**. Current and future applications to support enterprise operations rely on numerous middleware services. Examples of these services, in addition to the web technologies mentioned previously, are distributed object

technologies such as CORBA, drivers for remote database access, and a variety of other commercially available packages that support modern applications.

- **After-effects of Integrations**. Almost every application in modern enterprises ends up being integrated with others to provide faster and quicker services to the customers. While integrations are essential, they cause special headaches to the security administrators. For example, it is difficult to enforce security standards in systems that are results of integrations of several other systems that have widely different security attributes.
- **e-Business/e-Commerce Issues**. Both e-commerce and e-business require companies to be both more open and more closed at the same time. To benefit from e-business, supply chain management and other digital business processes of companies need to be open to outsiders such as customers, suppliers, and trading partners. Enterprise systems must also be extended outside the organization so that they can be accessed through wireless and other mobile devices. Yet these systems also must be closed to hackers and other intruders. The businesses need to straddle this fine line.

  Increased use of e-business has generally raised many new security issues. Consider, for example, the impact on the supply chains and customer relationship management of the companies listed in the sidebar, "Why Move Towards Digital Enterprises?" In addition, online purchase of items through credit cards exposes the customers to several privacy and fraud threats. An issue of particular importance is digital signatures and non-repudiation in e-commerce. In the traditional signed documents, the signer can repudiate the signature because of fraud or other coercions. The same may not be true with digital signatures.

These and other similar issues will drive the discussions in this book and will be illustrated through examples and case studies.

Israeli Government Moves Away From Microsoft Due to Security Concerns

Security is becoming a major factor in selecting software. In the past, software selection was based on factors such as cost, performance, scalability, and other features that did not necessarily include security. This seems to be changing. For example, the Israeli government suspended purchasing of Microsoft's productivity software in favor of open source alternatives, because of rising security worries over the Windows operating system. Many other governments, mostly in the Far East, have abandoned Microsoft applications in favor of open source offerings because open source software can be customized and "hardened" more easily. OpenOffice.org, an effort sponsored by Sun Microsystems to develop open-source versions of software that competes against Microsoft Office, is releasing a Hebrew language version of its software as part of a broad effort to develop localized versions of software.

Source: *information security news*, January 2004, http://www.infosecnews.com/

1.2.2 The IT Assets to be Protected

The main IT assets to be protected are naturally the applications, the services, and the data that support modern enterprises (see Figure 1-1). The main challenge is that these applications and services rely on a deep technology stack, shown in Figure 1-1, that needs to be protected. In particular, the following IT infrastructure building blocks need to be protected:

- Networks that provide the network transport between remote parties and are responsible for routing and flow/error control support. The networks may be the private value-added networks (VANs), the public Internet, and/or Extranets that utilize the wired or wireless transmission media.
- Computing platforms that consist of operating systems and computing hardware to provide the basic scheduling and hardware services. The computing platforms also include local system software services such as database managers, transaction managers, language translators, and utilities.
- Middleware that interconnects remotely located users, databases and applications. Middleware components are *business/industry unaware* software modules that provide a variety of services such as Web services, directory services, email, and remote data access services.

An interesting trend at present is to package a variety of IT building blocks into "application support environments" that can support the current and future breed of distributed applications. An example of such a dominant platform is Sun's J2EE (Java2 Enterprise Edition). Another example is Microsoft's .NET environment. These environments introduce their own strengths and weaknesses from a security point of view. Building a secure environment with so many technology building blocks with intricate interrelationships is not a trivial task.

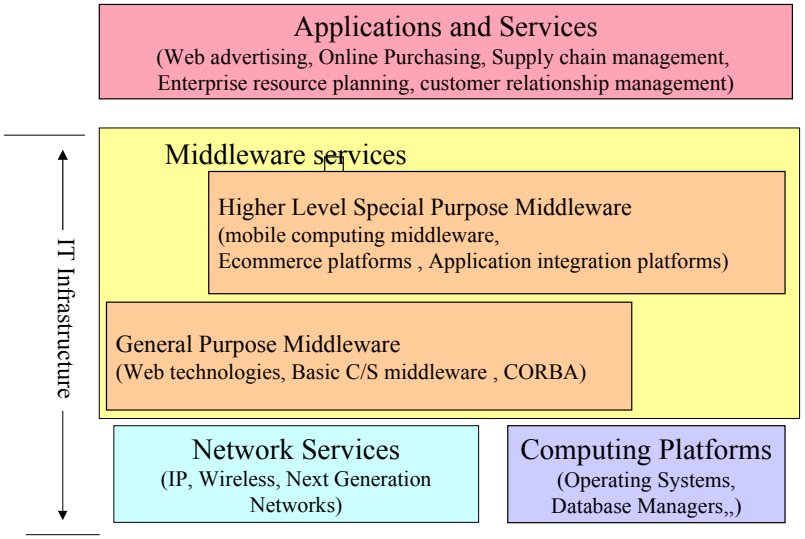


Figure 1-1: Modern IT Assets that Need to be Protected

1.3 Evolution of Security – The DARPA View at a Glance

Many of the ideas about security approaches are originating from the government work through research conducted through DARPA (Defense Advanced Research Project Agency). According to the DARPA OASIS (www.oasis.org) program, security approaches have evolved through several phases of research:

- **1GS** (First Generation Security): In this phase, the emphasis is on protection of the assets. Detection of security breaches is after the fact. Thus the main emphasis is on recovering from the attacks (i.e., information assurance).
- **2GS** (Second Generation Security): In this phase, the emphasis is on detection of the breaches before they can do any damage (or as quickly as possible).
- **3GS** (Third Generation Security): This phase involves research on building systems that can tolerate (survive) attacks and reconfigure themselves to adjust to the level of attack. These survivable systems are the main thrust of current and future research in security.

As work proceeds through various stages of security, we need to consider the following situations:

- **Hacking versus Assaults**: Hackers are basically "ankle biters" and irritants who can do damage to you, while assaults are much more dangerous because the aim of assault is destruction. The difference is analogous to pickpockets versus armed robbers. Higher level of protection is naturally needed against assaults.
- **Intrusion Tolerance versus Security:** Security generally means "protection" from malicious entities. However, intrusions may occur due to malicious or natural events. For example, a system failure due to a hardware problem, or an attack on the system, intrudes on your ability to do the work. Basically, intrusion is any undesirable/unauthorized activity that exposes, prevents and/or subverts a legitimate operation. ***Intrusion tolerance*** involves a combination of security and fault tolerance (Intrusion tolerance = security + fault tolerance). DARPA research has indicated that security and fault tolerance approaches contradict each other. For example, fault tolerance is achieved through replication; however, security is achieved through reducing replication (more copies are harder to protect).
- **Information Assurance versus Security.** Security concentrates on protection while information assurance (IA) deals with how to recover from security breaches. ***Information assurance*** is concerned with combining security with recovery; i.e., you not only protect the assets but also recover from the attacks. IA thus includes security plus backup/recovery, disaster recovery, and contingency planning. Generally speaking, assurance is the "ground for confidence that an entity meets its security objectives," where a security objective is defined as "a statement of intent to counter identified threats and/or satisfy identified organization security policies and assumptions."[2]

[2] Based on definitions by System Assurance Methodology (SAM) developed as part of the DARPA research.

1.4 Developing Security Solutions – A Framework for Discussion

1.4.1 Overview

Comprehensive security solutions are needed that protect the corporate IT assets by employing the latest security technologies to respond to the issues discussed above. More important than a detailed discussion of cryptography and individual security technologies, is the need to develop an architectural view that shows how modern corporate assets can be protected by using a combination of technical and organizational approaches. Figure 1-2 shows such a view and is the foundation of this book – the five blocks correspond to the five parts of this book (see the sidebar, "Book Outline").

Detailed analysis of requirements and development of an approach, discussed in part 1 of this book, are the first steps in building a security solution. Naturally, the evaluation and selection of the most appropriate security technologies, discussed in part 2 of this book, are vital to a comprehensive solution. The main purpose of IS security is to protect the IT assets (the databases, applications, computers, and middleware) plus the access path (the wired and wireless network firewalls) to these assets. How these assets can be protected by using the extant security technologies is treated in parts 3 and 4 of this book. Part 5 puts all the pieces together and concludes this book. The following sections capture the highlights of the topics discussed and are intended to provide a sneak preview of coming attractions.

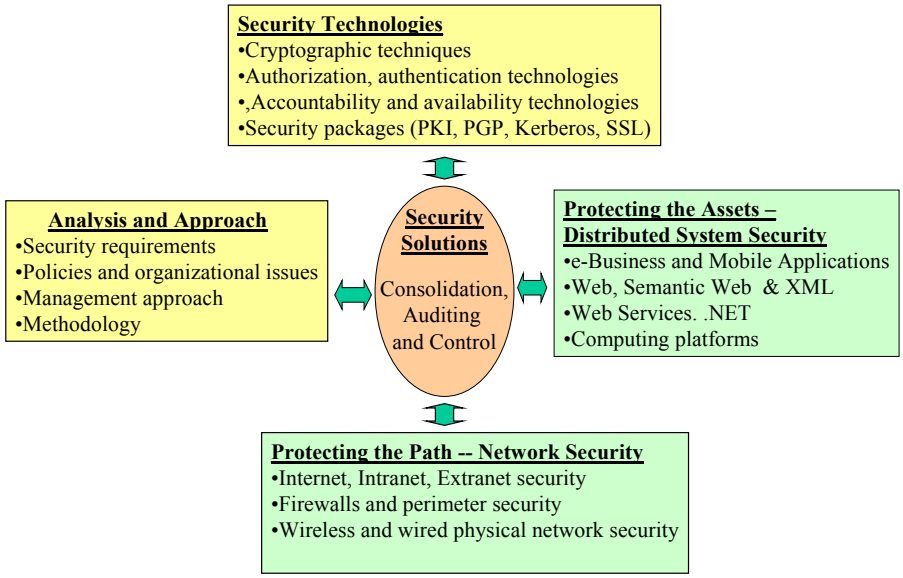


Figure 1-2: Security Solution based on a Systems View

Book at a Glance

PART I: ANALYSIS AND APPROACH

Chapter 1: Information Security in the Digital Age – An Overview

Chapter 2: Security Management: Polices, Requirements, and Organizational Issues

Chapter 3: A Systematic Methodology: Linking People, Processes, and Technologies

PART II: THE SECURITY TECHNOLOGIES

Chapter 4: Cryptography and Encryption

Chapter 5: Authorization, Authentication, Accountability, and Availability Technologies – The 4As

Chapter 6: Common Security Packages: PKI, VPN, SSL, PGP and Kerberos

PART III: PROTECTING THE PATH – DIGITAL NETWORK SECURITY

Chapter 7: Overview of IT Assets in Modern Digital Enterprises

Chapter 8: Network Security, Internet Security, and Firewalls

Chapter 9: Wireless Security: Wi-Fi, Cellular and Satellite Security

PART IV: PROTECTING THE SITES – DISTRIBUTED SYSTEM SECURITY

Chapter 10: Web, Semantic Web, and XML Security

Chapter 11: Modern Distributed Platform, Web Services and .NET Security

Chapter 12: Application Security: Protecting e-Commerce and Mobile Applications

PART V: PUTTING THE PIECES TOGETHER

Chapter 13: Audit and Controls for Security

Chapter 14: Building a Security Solution – The Wrapup

1.4.2 Analyzing Threats and Developing an Overall Approach

The purpose of security is to protect a system against potential attackers who exploit system vulnerabilities. Security requirements to protect the IT assets are established as the first step in building a security solution. These requirements identify the most valuable and critical assets to be protected. The requirements must be able to take into account the external factors (realities of life at national or international levels) that drive

security initiatives in modern enterprises, as well as organizational requirements that are different for different organizations. For example, a PC store has different security requirements than the Pentagon. Similarly, healthcare industries have to comply with numerous external regulations that do not apply to manufacturing organizations.

After these security requirements, next steps typically involve a study of vulnerabilities of a system, identification of the type of attacks that could exploit the vulnerabilities, and introduction of circumventions (countermeasures) to handle the threats. Vulnerabilities, threats, and circumventions can be discussed in terms of privacy, integrity, authentication, authorization, accountability, and availability (abbreviated as ***PIA4)***:

- ***Privacy*****:** assure confidentiality of information (e.g., no one other than the authorized people can see the information) when transmitting it over a network or storing it in a storage device.
- ***Integrity:*** assure retention of information (i.e., no unauthorized modification) during transmission or storage.
- ***Authentication:*** identify for certain who is communicating with you (i.e., make sure that you are who you say you are).
- ***Authorization*** **(Access control):** determine what access rights that person has (i.e., can you only read given information or can you also update, delete, add information).
- ***Accountability:*** assure that you can tell who did what, when; and convince yourself that the system keeps its security promises.
- ***Non-repudiation (NR),*** the ability to provide proof of the origin or delivery of data, is an important aspect of accountability. NR protects the sender against a false denial by the recipient that the data has been received. It also protects the recipient against false denial by the sender that the data has been sent. In other words, a receiver cannot say that he/she never received the data, and the sender cannot say that he/she never sent any data.
- ***Availability:*** assure that the users can use the system when they need to. Attacks such as denial of service attempt to minimize the system availability.

These attributes of security can be used to define the level of security (protection) exercised on different corporate resources. Table 1-1 shows an example. The entries can be low/medium/high instead of yes/no.

Table 1-1: Example of a Security Profile

Resources	Privacy	Integrity	Authentication	Authorization	Account-ability	Availability
Customer Database	Yes	Yes	Yes	Yes	No	Yes
Payment System	Yes	Yes	Yes	Yes	Yes	Yes
Web Advertising	No	Yes	No	Yes	No	Yes
Web Server	Yes	Yes	Yes	Yes	No	Yes
Corporate Network	Yes	Yes	Yes	Yes	No	Yes

A management approach is needed to develop organizational policies, roles, responsibilities, and training programs before choosing security technologies (this issue

is ignored by several academics). This approach must also include how the risks of security exposures will be managed and how the company can survive different types of attacks. The management approach must be based on a systematic methodology that combines the organizational and technical approaches into a solution.

The three chapters of Part 1 provide more details on these topics.

1.4.3 Security Technologies at a Glance

A wide range of technologies and techniques have been developed over the years to deal with the PIA4 vulnerabilities mentioned above. Here are the key players at a glance.

- User logon and password is one of the oldest and still most commonly used technologies.
- Encryption is another technology that has been used for a number of years to mask messages so that adversaries cannot see/modify the messages. Encryption is generally discussed in terms of two approaches: a) Private key (symmetric) encryption schemes in which the same algorithm is used by the sender to encrypt the message and the receiver to decrypt it, and b) Public key (asymmetric) systems in which the encryption algorithm E and the decryption algorithm D are different - hence the name "asymmetric."
- A digital signature is used to authenticate the source of a message. It is based on the public key encryption technology.
- Message digesting is used to make sure that a certain message was not changed along the way between the sender and the receiver.
- A digital certificate binds an entity's identification to its public key and is issued by a Certification Authority (CA).

In reality, if you want to secure a system, you do not get individual technologies. Instead, numerous security packages are commercially available at present that integrate different security technologies. Examples of some of these packages are:

- VPN (Virtual Private Network) – a package for encrypting the messages being sent over the public Internet.
- SSL (Secure Socket Layer) – a package commonly used for secure communications between Web browser and server.
- Public Key Infrastructure (PKI) – a family of technologies that are based on the public key cryptography and contain the facilities to store and manage certificates (i.e., the ability to issue, revoke, store, retrieve, and trust certificates).
- PGP (Pretty Good Privacy) – a popular program, available on the Internet, that uses public-key cryptography to authenticate users to each other without the use of certificates.
- Kerberos (http://ww.mit.edu/kerberos/) – an open standard designed to provide strong authentication by using secret-key cryptography.
- Verisign (www.verisign.com) – security solutions for certificates, secure messaging, wireless systems, and payment systems.
- Tivoli (www.tivoli.com) – provides a set of security services under the IBM Tivoli Access Manager that controls both wired and wireless access to applications and data in IBM environments.
- Microsoft's Passport Service – a PKI system to provide single-signon for the .NET environment.

See Part 2 of this book for additional discussion of security technologies and packages.

1.4.4 Securing the IT Assets and the Access Paths – A Quick Glance

IT assets (databases, applications, computers) as well as the access paths (the wired and wireless networks) to these assets need to be protected. From an overall system point of view, security is needed at all levels (network, middleware, application) by using the most appropriate security technologies and packages (see Figure 1-3). Security is needed at these different levels since security at each level fulfills different requirements. Let us briefly review the security at various levels (details are provided in Part 3 and 4 of this book).

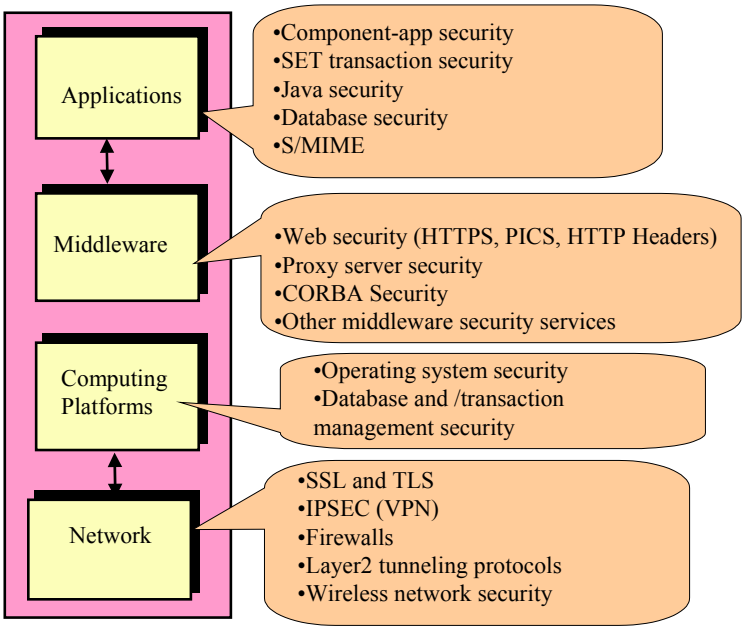


Figure 1-3: Levels of Security

Network security protects information when it is in transit between end points. For example, even if a database is secured through IDs and passwords, the transmission of the data between a remotely located user accessing the database is not protected automatically. To protect against eavesdropping and integrity attacks, the network traffic can be encrypted at the packet level through VPN (IPSec) or at the transport level (SSL-Secure Socket Layer). "Firewalls" and "gateways" are also erected to protect and regulate network traffic. Many security issues exist for wireless networks because all wireless networks (wireless LANs, cellular networks, satellites) use air as a transmission medium. This medium is much easier to intercept – you basically need an antenna – and hence the need for better security.

Traditional approaches to host security include operating system and database management security. Middleware security is a relatively new player in host security and needs special attention. Simply stated, middleware is business-unaware software that connects applications, users, and databases across machines. Common examples of middleware services are Web browsers, Web servers, email packages, and CORBA. A more recent example of popular middleware services is Web Services, at the core of Microsoft's .NET and Sun's J2EE platforms. Middleware services play a dual role in security – they imbed security but also need to be protected themselves. CORBA is a good example – it imbeds security software that assures that CORBA applications are secure, but CORBA software itself also needs to be protected.

Databases and applications are the most valuable IT assets for most organizations. A variety of security approaches exist at the application level, in which case authorization controls are used within applications to regulate access to specific data, and cryptographic infrastructures are built to strongly authenticate users and provide confidentiality. Examples of application-level security is provided by database managers, Java security, and SET (Secure Electronic Transactions). In particular, applications themselves provide access control and strong user authentication.

Security must be considered at all levels. Securing a higher layer while keeping lower layers unsecured makes the system vulnerable to intrusions from the lower layers. In general, lack of security at a certain layer might compromise the overall system even if other layers are secured. Consider, for instance, a system where the application data is secure, but is transmitted over an insecure network. In this case, the overall security of the application could be suspect. Specifically, application security protects application data (e.g., database security mechanisms allow the data to be stored on the hosts in a protected manner) and system resources (e.g., Java Security), while SSL protects data during its transfer on the network.

1.4.5 Building and Deploying a Security Solution

The various pieces (requirement analysis, threat analysis, policies, procedures, technologies, and specific approaches to protect different IT assets at different levels) need to be integrated into a solution that can be built, deployed and controlled. The solution typically consists of: a) documentation of the requirements, threats and policies, b) a solution architecture that puts all the technical pieces together, and c) a control and audit approach to assure continued secure operations. Figure 1-4 shows a sample solution architecture for a Web-based system that allows users to access corporate systems through a variety of wired and wireless devices. Let us review it briefly.

In developing a solution architecture, several factors need to be taken into account. Basically, it is important that the business logic of a Web application runs on a server and not on the client. The Web application server can be used to integrate access to resources (databases, etc.), which provides greater security of the resources. In addition, applications and databases should be protected by using network filters ("firewalls"). A good design protects the Web server (providing presentation services) behind an outer firewall, and the remaining servers (supporting business logic) behind a second, inner firewall. This structure, shown in Figure 1-4, is known as a demilitarized zone, or DMZ. In most cases, a Web server sits alone in the DMZ, handling requests from the Web and passing them along to the secure intranet network. The applications and internal business

systems behind the inner firewall contain all the remaining business logic and data of the application. In addition, you can gain performance benefits by caching frequently requested data inside the DMZ rather than retrieving it from back-end systems each time it is requested. However, machines in the DMZ are known to be at higher risk. In addition to the DMZ, you also need to consider security of clients. For example, mobile devices typically need another level of security before they can enter the DMZ.

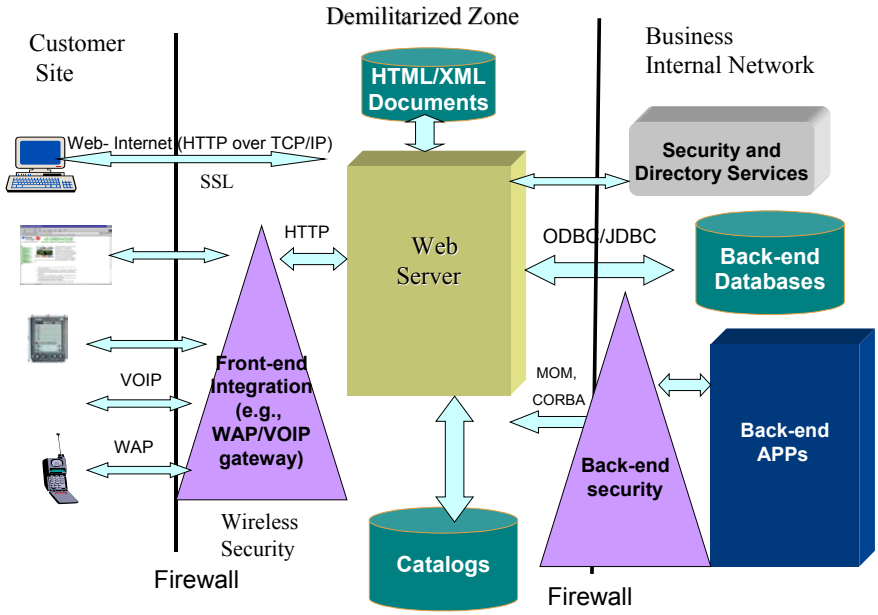


Figure 1-4: Sample Security Solution

A question that plagues many security managers and corporate executives is how to prevent and detect attacks so that appropriate responses can be developed in time. A common approach is to develop **honeypots** that are built especially to be probed, attacked or compromised by the intruders. These devices are called honeypots because they are expected to attract the bees, flies, and worms – the hackers and intruders. The idea is to have attackers spend time and resources attacking honeypots, as opposed to attacking corporate systems. See the sidebar, "Cheating the Cheaters – Honeypots and Other Diversions."

It is not enough to develop solutions once and then forget about them. **Controls and audits** are needed to assure *continued* secure operations. For example, suppose you develop a highly secure solution in 2004 with the best policies, procedures, and technologies for mobile applications. How do you know that the choices and decisions you have made will be followed in 2005, 2006 and 2007? In addition, how do you assure that the decisions made now are good enough and will last through the technological as well as organizational changes in the next several years? Audits and controls are a good mechanism for smooth and effective operations for several years to come.

Although audits and controls have been well established for many years, new information technologies raise new issues that have not been traditionally thought of in the control procedures. Specifically:

- XML and its reliance on external schemas requires new procedures for edit checking. Not only the XML document itself, but the schemas must also be controlled to make sure that the processing is not tampered with.
- Web Services requires new controls for the services that can be directly invoked over the Internet through universal directories.
- Wireless networks and mobile devices present many new challenges for control. For example, in the past it was possible to install terminals in a physically secure area for restricted access. This is simply not possible with the highly mobile workforce of today that accesses corporate information over cellular networks.
- Application servers such as IBM's Websphere and Micrososft's .NET support many applications. These new infrastructure components need to be properly controlled.

See Part 5 for more discussion of these topics.

Cheating the Cheaters – Honeypots and Other Diversions

Honeypots are diversionary devices that are developed especially to be probed, attacked or compromised by the intruders. Here are some examples:

- Fake websites are set up by companies with misleading or wrong information to attract the attackers. These sites may pose to provide restricted, expensive or illegal information free of charge.
- Movie producers, tired of free distribution of the latest movies over the Internet by hackers, are supporting fake movie sites. The idea is that a freeloader finds this free movie site and downloads what appears to be a good movie – but instead gets a blank screen or some junk. This is especially irritating to someone who waits for hours to download some movies and finds nothing of value. This could potentially discourage the freeloaders.
- Music producers, also tired of free distribution of music, are increasingly resorting to fake music sites. Some of these sites also attempt to entrap the freeloaders.

Although the main idea of honeypots is to cheat the cheaters, they have become valuable resources to study the identity and behavior of intruders. Due to their role, commercially available honeypots have been developed. These honeypots allow companies to fake email sites, databases, websites, and other resources.

See Chapter 14 for a detailed discussion of honeypots.

1.5 Security in Electronic Commerce – An Example

1.5.1 Overview

To illustrate what we have discussed so far, let us build a sample security architecture for an e-commerce (EC) system that allows users to access a catalog and then place orders online (see Figure 1-5). The online orders are placed through a variety of wired and wireless devices, and many back-end applications and databases such as payment systems and inventories get involved in processing the orders. The main idea is to walk through various choices through an example. The details can wait; let us just see how various pieces fit together in developing a security solution.

In EC, risks need to be analyzed, and information must be protected and its integrity maintained at the sites where it exists and when it is transmitted. In addition, the encryption keys themselves need to be protected; and audits/controls are needed for continued safe operations.

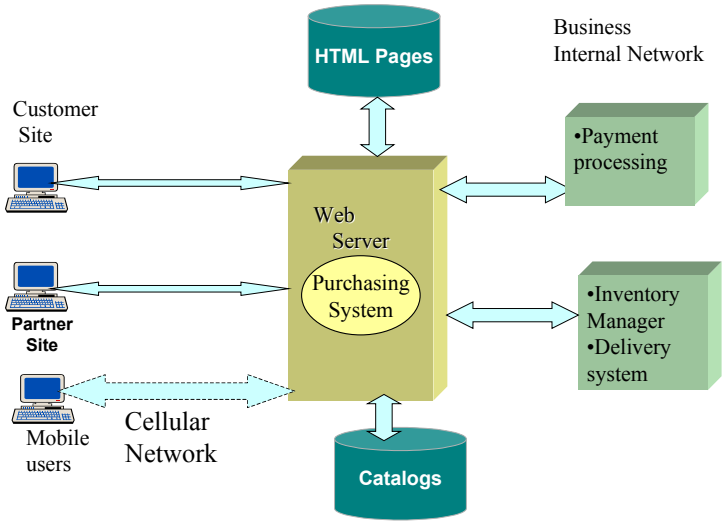


Figure 1-5: Sample e-Commerce Site

1.5.2 Risk and Threat Analysis

Information security is a major control issue for companies engaged in e-commerce. The commerce-related data of buyers and sellers must be kept private when transmitted electronically. The information being transmitted also must be protected against being purposefully altered by someone other than the sender. Otherwise, for example, item purchases and stock market execution orders would not accurately represent the wishes of the participants. In addition, the data involved in online buying and selling must be stored on secure sites with proper protection. Otherwise, intruders could, for example, modify data regarding who purchased what items at what prices. Chapters 2 and 3 discuss various threats and risks in more detail.

1.5.3 Analysis of Encryption Technologies

Encryption is used to protect sensitive EC information transmitted over the Internet and other networks. For example, credit card information is encrypted for protection. Encryption basically scrambles messages to prevent unauthorized access to, or understanding of, the data being transmitted. A message is encrypted by applying a secret numerical code, called an encryption key, so that it is transmitted as a scrambled set of characters. In order to be read, the message must be decrypted (unscrambled) with a matching key. The old encryption systems, called private or symmetric key systems, use the same key for encryption and decryption.

Over the years, several alternative methods of encryption have been developed. However, "public key" (also known as "asymmetric key") encryption is quite popular and is used regularly in EC. Public key encryption, illustrated in Figure 1-6, uses two different keys, one private and one public. The two keys are mathematically related so that data encrypted with one key only can be decrypted using the other key. To exchange messages, communicators first create separate pairs of private and public keys. The public key is kept in a directory so that others can read it while the private key is kept secret. Suppose that the buyer wants to send her credit card information to the merchant. The buyer encrypts the card information with the merchant's public key. On receiving the message, the merchant uses his or her private key to decrypt it. No one else knows the private key except the merchant, ensuring that the message was kept private during transmission.

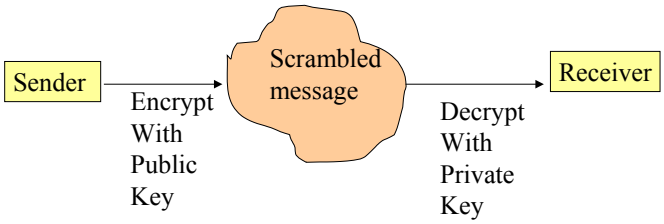


Figure 1-6; Public Key Infrastructure

A number of encryption standards exist. SSL (secure sockets layer) is a popular protocol for secure information transfer over the Internet and is quite commonly used in EC. It allows client and server computers to manage encryption and decryption activities as they communicate with each other during a secure EC session.

Besides privacy, authentication and message integrity is needed in EC. Encryption not only helps protect transmission of payment data, such as credit card information, but also addresses problems of authentication and message integrity. Authentication is important in EC because the merchants need to know that the buyers are who they claim to be, and vice versa. Digital signatures used for authentication currently have the same legal status as those written with ink on paper. A digital signature uses public-key encryption to attach a digital code to a message, and performs a function similar to a written signature.

Another technology used for authentication in EC is digital certificates. Digital certificates are data files used to establish the identity of people and electronic assets for protection of on-line transactions (see Figure 14-6). A digital certificate system uses a

trusted third party known as a certificate authority (CA) to validate a user's identity. Basically, a digital certificate is similar to a passport that has been issued by a CA.

Chapters 4, 5, and 6 discuss the various encryption technologies and the packages in more detail.

1.5.4 Transmission Protection – Network Security

When EC data travels outside of a secure system environment, such as the customer network, it needs to be protected so that the policies governing its use cannot be violated. Secure communications, ensuring data privacy, data integrity, and origin authentication, are an important aspect of information protection while in transit.

A traditional approach to achieve network security is to use private networks. For example, on-line commerce continues to be handled through private EDI (Electronic Data Interchange) software usually run over VANs (value-added networks). VANs are relatively secure and reliable but are expensive, easily costing a company $100,000 per month. In addition, VANs are inflexible, being connected only to a limited number of sites and companies. For example, a merchant can only engage in EC with the customers on the VAN. Naturally, the public Internet is the network technology of choice for EC. For example, a merchant in Singapore can reach buyers in England, US, and Kenya over the Internet. However, the public Internet is insecure. Examples of the technologies used for secure communications over the Internet are:

- VPN for secure messages over physical network connections between computers
- SSL for secure messages between EC buyers and sellers
- Firewalls to protect specific resources involved in EC
- Intrusion detection systems for monitoring and detection of intrusions

VPN and IPSec. Virtual Private Networks (VPN) are private networks (e.g., networks internal to corporations) that use public communication infrastructure. In other words, you setup a private network over a public network by using encryption. VPNs use IETF IPSec (RFC 2401) and related standards to transport encrypted messages over shared networks. IPSec provides security at the packet level, instead of security at the application layer. It encrypts and signs headers and/or data parts of IP Header. It provides security without requiring changes to applications and thus is suitable for Virtual Private Networks (VPN). VPN differs from SSL in that it creates a secure channel between two TCP/IP hosts over which multiple TCP/IP connections can be established. Each TCP/IP session itself may or may not use SSL. A VPN, shown in Figure 1-7, provides dedicated, secure paths over a network that is shared by other users. The secure paths, called "tunnels," are set up between a point of presence (POP) and a terminating device on the destination network.

SSL. The Secure Sockets Layer (SSL) protocol uses encryption and authentication techniques to ensure that communications between a client and a server remain private, and to allow the client to identify the server and vice versa. SSL runs on top of TCP/IP and manages secure messaging on the network. SSL client and server negotiate the encryption scheme and key size. SSL is currently used heavily to protect the traffic between Web clients and servers. It uses RSA (Rivest, Shamir, and Adleman) public encryption for key session negotiation and DSA (Digital Signature Algorithm) for session encryption.

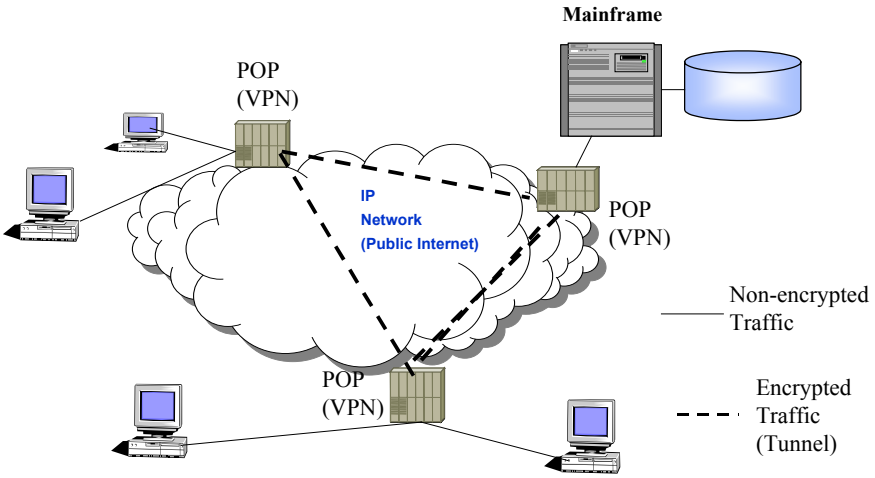


Figure 1-7: A VPN

Firewalls are the network filters that police *who* enters and leaves an enterprise network and *what* gets in and out. As growing numbers of businesses expose their networks to Internet traffic, firewalls are becoming a necessity. A firewall is essentially a software package that is installed on network routers. This software checks each IP packet and determines if it should enter the system. The firewall controls access to the organization's internal resources by acting like a gatekeeper that examines each user's credentials before allowing access to the network. It protects the enterprise "perimeter" by identifying names, Internet Protocol (IP) addresses, applications, and other characteristics of incoming traffic. The firewall checks this information against the access rules that have been programmed into the system by the network administrator.

Firewalls provide a logical and physical separation of the public Internet and internal IT systems. The firewall prevents unauthorized communication into and out of the network, allowing the organization to enforce a security policy on traffic flowing between its network and the Internet. A good security design generally has two firewalls: an outer firewall that exposes some services to the outside world and a second, inner firewall, that keeps the inner resources. The zone between the two firewalls, as discussed previously, is known as a demilitarized zone, or DMZ.

Intrusion Detection Systems (IDSs). These tools and services are commercially available to protect against suspicious network traffic. Used in addition to firewalls, intrusion detection systems provide monitoring tools that can be placed at the most vulnerable points of corporate networks to continually detect and deter intruders. IDS software looks for known problems such as repeated tries with bad passwords, checks to see if important system files have been removed or modified, and sends warnings of misbehaviors. IDS software examines events as they are happening and may shut down a particularly sensitive part of a network if it receives unauthorized traffic.

Most EC sites at present support firewalls and SSL. VPNs are essential for wireless access because the physical wireless network is easier to tap and disrupt. See chapters 8 and 9 for detailed discussion of wired and wireless network security.

1.5.5 Site Protection

EC information must be protected at the sites where it exists. Access control (allowing authorized users to access needed data) protects data at various sites. Most database managers have security features that allow only authorized users to access needed data. In some cases, data is encrypted and stored for additional security.

A wide range of approaches can be used to protect EC sites, ranging from operating system "hardening" to email security (see Part 4 of this book). The following are of particular importance:

- XML security
- e-Commerce platform security
- SET
- Server-side "hardening"

XML Security: XML is a powerful and highly flexible markup language for documents containing structured information. It is very popular at present in e-commerce for describing purchase orders, customer information and other information needed for on-line trade. XML has, however, introduced several security concerns. The main concern is that XML validity depends on an externally defined schema (see Chapter 10 for details). Thus not only the XML documents but also the XML schema needs to be protected. A straightforward way of securing an XML document and its schema is to encrypt both. However, different parts of the same XML document frequently need different levels of security, because different groups of users may need different parts of the XML document. For example, a merchant needs to know a buyer's name, the items bought, and the shipping address, but does not need the credit card information. However, the bank needs to know the credit card information but has no interest in the goods bought. Different standards such as XML Encryption and SAML (Security Assertion Markup Language) are being developed (see Chapter 10 and 11).

e-Commerce Platform Security. Since the late 1990s, several technologies have been packaged together by vendors as ***"middleware platforms" or "application servers"*** for special purposes**.** For ***e***xample, e-commerce platforms such as WebSphere (www.ibm.com), Broadvision (www.broadvision.com), and OpenMarket (www.openmarket.com) are available that combine Web, mobile access, cataloging, payment, order processing and other services together for e-commerce. If an e-commerce application is built by using these platforms, then the security features provided by the particular platform need to be considered (see Chapter 11 for details).

SET - Many credit card payment systems use SSL for encrypting the credit card payment data. However, SSL does not verify that the purchaser is the owner of the card being used for payment. The Secure Electronic Transaction (SET) protocol was developed jointly by Visa, MasterCard, IBM, and other technology providers to protect the transfer of bank card payment information over open networks like the Internet. A SET user acquires a digital certificate and SET-enabled digital wallet. The wallet and certificate specify the identity of the user and the credit card being used. This information is used to authenticate and encrypt the traffic. See Chapter 12 for details about SET.

Server-Side Hardening. A common attack on e-commerce sites is launched by using weaknesses of the server-side programs. These weak programs can be test programs that were left on the system inadvertently such as a default CGI (Common Gateway

Interface) script that the attackers invoke from their browsers. The attackers either try to gain privileged status through these programs, or introduce other viruses. The best way to defend against such attacks is to "harden" the server-side programs by deleting all untested and flawed code on the Web servers. See Chapter 12 for more details.

1.5.6 Security Solution, Audits and Controls

Figure 1-8 shows a sample security solution that maps the choices discussed previously to the initial configuration shown in Figure 1-5. As illustrated, a firewall has been placed between the purchasing site and the back-end systems; SSL is used to establish secure sessions; and SET is used for the payment system. VPN is used mainly between the partner sites and the mobile users, due to added security requirements (partners place larger orders, and wireless networks need extra protection). VPN could be used for regular customers also. For site protection, it is also important to "harden" the purchase site by installing the latest virus control software.

Assuming that the online purchasing system is built by using Microsoft Commerce Server, then the security features of this e-commerce platform will be included in this solution. A honeypot, not shown in the diagram, may be developed to divert the intruders.

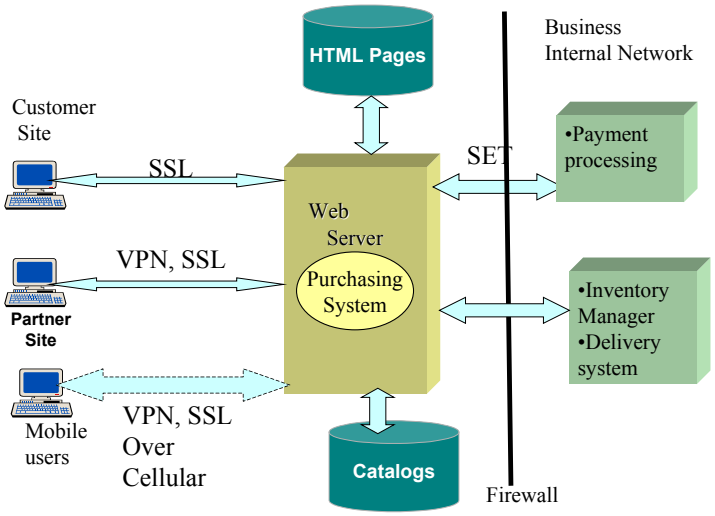


Figure 1-8: Sample Security Solution for an Online Purchasing System

Proper controls and audit procedures are also needed for a continued secure operation of this e-commerce site. Unfortunately, the term "audit" scares most people. There are different types of audits – the most feared is the tax audit by the IRS. Our interest is in IT audits that diagnose the effectiveness of controls needed for efficient and secure operations. Proper controls, sometime needed for compliance with laws and regulations, can also be used as strategic tools to increase efficiency of processes, improve

profitability of enterprises, and increase reliability of financial data.[3] Examples of these controls are the policies and procedures that control and restrict the access to sensitive applications, databases, and corporate network segments to minimize frauds and assaults. While controls are needed to establish a secure and efficient enterprise, security audits are needed to assure that the controls are actually being used. Information security audits determine how the privacy, integrity, and availability of an organization's information is being achieved and what can be done if it is not. See Chapter 13 for discussion of security audits and controls.

In e-commerce, the paths as well as the sites need to be properly protected, controlled, and audited. In addition, protection of the keys that in turn are used to protect the assets is also important. Private keys and shared secrets, once acquired, must be protected. End-to-end security must include consideration of the security of the end user device. Private keys stored on a personal computer disk file may be stolen via access to the file system or outright theft of the device. Security can be enhanced by the use of smart cards. Another approach is to use a security chip embedded in end-user systems. In addition, server-side hardware devices can provide tamper-resistant key storage as well as assistance for encrypting and decrypting messages, public/private key operations, etc. that require heavy computational load.

1.6 Short Case Studies of Security

The following case studies were collected by the students of my class on "Security and Information Assurance," taught at the Fordham Graduate School of Business (Summer, 2002). The names of the contributors are Tracy Brown, Rebeca Cates, Michael Collins, John Coyle, Michael Fazio, Christopher Freiler, John Geraghty, Rita Ghei, Kevin Kline, Mary McNally, Tammie Min, Thomas McGinley, John Morris, Pankaj Navathe, Mitch Rothman, and Viktoryia Petrashova.

1.6.1 Standard Chartered Bank: Remote Access Disaster Recovery/Business Continuity Plan

1.6.1.1 Context and Background

Standard Chartered is a British emerging markets bank with a focus on Asia, Africa and the Middle East. Its wholesale banking unit, known as Corporate & Institutional, is managed globally from Singapore. A large portion of the bank's Asian business is driven from the New York (Americas) office. From New York, Standard Chartered helps Fortune 500 customers like Coca Cola, Wal-Mart and Disney finance their operations in Asia.

The bank relies upon a Lotus Notes-based system for email communication and for housing the bulk of the bank's credit and revenue databases.

---

[3] Bell, T., et al, "Auditing Organizations Through a Strategic-Systems Lens," KPMG Publication, 1997

Before September 11, 2001, it was very difficult to use the email application of Lotus Notes successfully from a remote location. Remote access to critical databases was virtually impossible.

After September 11, 2001, Standard Chartered Bank lost its Americas office in 7 World Trade Center. Everyone survived, fortunately, but just about every computer and server was lost. While the operations department had a disaster recovery plan established to continue business in a limited capacity after the disaster, the Americas front office (approximately 80 people) were left sharing 2 computers at the small disaster recovery site in Jersey City.

It took several months for the front office to get back to business as usual. A decision was made by local management to purchase laptops for every critical front office employee to keep at home. The laptop strategy would distribute risk geographically and was considered to be safer (people wouldn't have to leave home) in the event of another tragedy. In addition, people who needed to work from home would now be able to gain access to bank systems from home.

The strategy, while very compelling, leaves some unanswered security questions. How can the bank insure that its valuable information is secure with the new remote strategy?

1.6.1.2 Security Problem

Credit limits are proposed and approved via a Lotus Notes-based system called Fasttrack. Digital signatures authenticate that the person proposing/approving limits is who they claim to be. What, if anything, needs to be modified with the current system as we move toward remote access?

Connectivity: What are the security risks of transferring confidential bank data via phone lines (dial-up connection) versus DSL or Cable Modem?

1.6.1.3 What is at risk?

The bank's confidential customer data is at risk. It could be detrimental if one of the customers or competitors were able to access this information. Also, there is a concern with regard to rights/credit approval authorities getting into the wrong hands (e.g., they wouldn't want someone with access to the Regional Credit Officer's laptop to be able to approve a $100-million loan arbitrarily just because he or she had physical access to his laptop at home).

1.6.1.4 Problem Categorization

Management: Who can access what systems and databases remotely?

Network: What concerns are there with regard to accessing the bank's LAN/GWAN network remotely?

Web: A soft copy of the bank's Disaster Recovery Plan will be kept online along with employee contact information on a password-protected website. There are a number of ASPs that the front office uses (e.g., Moodys.com). Are there any remote access issues there? Will everyone access the bank's systems via the web or via a dial-up connection?

Database: Should there be any limits with regard to database remote access (printing limitations, read only)?

1.6.1.5 Solution Approach – What should be done?

Security Awareness: Security policies need to be established and implemented. Procedures and guidelines must be put in place to enforce the policies. Bank managers and employees need to be told about these policies.

One person from each business unit has to be put in charge of his or her team's security management program. Checks need to be made on the program periodically.

After key threats are identified, a training program should be implemented to teach users of the new remote access system how they can protect the bank from becoming vulnerable to newly identified threats associated with remote access.

Standard Chartered (Americas) needs to develop a security architecture that satisfies the requirements in terms of organizational policies, an awareness program, and enabling technologies.

The bank is looking at a remote networking application called Shiva that offers users access to bank systems via the Internet. The Shiva system is expected to ensure security of bank systems through the use of single-user logons and strong authentication. Shiva also enables administrators to centrally manage the access rights of remote users.

1.6.2 CNN Denial of Service (DoS) Attack

In February 2000, the cable network CNN was victimized by a denial of service attack (a denial of service attack is a situation where hackers flood a system with numerous useless messages that tie up the system, resulting in a possible loss of service). The CNN website (www.cnn.com) was shut down for approximately two hours as a result of hackers who flooded the servers, thus rendering the website inaccessible to the general public. At the time, these website attacks were considered to be the most severe to date. These incidents highlighted the need for greater study into the field of information assurance and security.

In terms of CNN and media concerns, the attack proved that media companies were also susceptible to electronic sabotage. In essence, these attacks threatened the competitive advantage that news websites possess over other forms of news media – the ability to break news at all times of the day. If CNN's website could be put out of commission for extended periods of time, people would no longer rely on cnn.com to report news in a timely manner. This issue was of paramount importance to CNN. Also related to CNN and denial of service was the loss of advertising revenue on the site. If viewers are kept off the site, advertisers can demand a refund or credit on their account. CNN will then be required to make good on the advertising space that was lost due to the site shutdown.

Another concern that CNN and other news websites must have considered after the assault was that if hackers could keep people out of their websites, could the hackers also break in and revise or delete news copy? This is an even graver concern for media organizations. CNN would lose a tremendous amount of credibility if people could access their website and change news stories. For this reason, CNN must implement tighter security around their website to safeguard against hackers that can disrupt and discredit their hard work.

Let us look at denial of service somewhat more closely. Unlike most other types of "hacks," a denial of service attack will not usually result in the theft of information or

other specific security losses. Instead, a denial of service attack results in either loss of service or extremely slow response time on a website. This can be extremely damaging because it can frustrate consumers and hurt the reputation of a website in terms of reliability; and if the site is revenue-generating, it can potentially result in the loss of sales.

Specifically what happens is that a constant stream of requests is sent to a target with the intention of overloading it. The information is sent to the target in small packets of data called "pings" which are used as a signal between two computers. The attacker sending the "pings" lies about their real address so the target computer is unable to return the ping and make any connection. As a result an enormous amount of junk traffic floods the computer beyond its capacity, causing the website to become unavailable.

The denial of service attack that hit CNN Interactive on February 8, 2000 had serious impact on the site and overall caused a lot of risk to the organization, in regard to assuring their customer base that the site is secure and reliable. CNN Interactive provides content that needs to be very accurate and as up-to-date as possible in order to meet the needs of their customers. On this day the content that was served was very inconsistent and out of date, and overall the site was extremely slow. In all the hackers affected the news site operations for nearly two hours. The situation could have been a lot worse for CNN had it lasted longer than two hours. When sites like CNN are inaccessible it means a loss of both integrity and revenue for the firm.

In the instance of a company heavily dependent on its website for revenue and survival, how management responds to a DoS attack may well determine if the company can survive. Since the network is by definition overloaded by a DoS attack, management must rapidly recognize that the attack has begun, and either eliminate the superfluous packets choking their network lifeline or reroute the traffic to a backup network. The databases that companies use should remain unaffected by the DoS attack except inasmuch as the people who need the information within the database will be unable to access or use it. Unless there is something more nefarious attached to the DoS packets, once the traffic is sorted out, cleaning up the database is relatively straightforward, albeit time-consuming and therefore expensive. Applications accessed through the network affected by the DoS attack will be slowed – if not outright crashed – by the overwhelming network traffic. If the applications are critical to running company operations, especially in virtual companies such as Sun Microsystems, the entire company, not just the website, will come to a halt.

Though the concept of the DoS attack is straightforward, it seems that there are only three possible strategies to prevent DoS attacks in the future. The first strategy involves using address filtering at edge routers to detect and prevent large numbers of fake packets from entering the network. However, such a fix is expensive and thus far has not been widely used due to fears of its longevity. Second, UUNET and Cisco are working on reverse path forwarding protocols to be sure packets are coming from appropriate networks. Unfortunately, though RPF will be cheaper, it is still on the drawing board. The third and only truly foolproof manner of preventing DoS attacks is to beat the hackers to the punch – by shutting down your own website and handling all transactions in person. But this is not acceptable.

1.6.3 Case Study: Power and Energy

Maxwell Utilities,[4] a leading electric utility company and member of the Fortune 500, recently began a large-scale restructuring effort in order to compete successfully in a deregulated environment. Company executives realized that they needed to increase their focus on information security to reduce business risk exposure during the restructuring effort.

A corporate wide area network (WAN), and an energy management system (EMS) supported the majority of operational applications. Additionally, power plants had separate networks to control generation operations. The company's reputation, consumer confidence and, in the case of the EMS and power plant systems, national security, were all at stake. A powerful information security solution was crucial.

In order to operate efficiently, the security partner needed to provide policies that were transparent to Maxwell Utilities' business processes, updated on a regular basis, and unobtrusive to the company's end users. The company considered several leading vendors, and ultimately chose Riptech Security Professional Services to provide planning and assessment.

The security problem was the fact that their internal networks would be extremely vulnerable to attacks while the reconstruction effort was taking place. Since information security is a key aspect in their ability to stay competitive, they needed to protect themselves from any security breeches.

Furthermore, Maxwell Utilities required a partner with experience in performing security audits and assessments of both corporate and EMS systems for large utilities. The partner needed a firm understanding of the unique security risks presented by industry restructuring and deregulation.

Riptech characterized the problems as follows:

- The network architecture was dissected to identify and exploit vulnerabilities in the corporate network.
- The internal databases, systems and network administrators were assessed to determine vulnerabilities that are likely to threaten the business activities or cause denial of service.
- All entries to the network (via remote login, Web, firewalls, etc.) were analyzed to determine any "holes" that would compromise the security of the firm.

Riptech consultants identified a File Transfer Protocol (FTP) server located at the offices of a newly acquired company. The FTP server was accessible from the Internet and permitted access to all Maxwell Utilities systems. Consultants reported the server location to Maxwell system engineers, who promptly reconfigured the server to eliminate the possibility of a security breach.

Riptech consultants identified the Internet Information Service (IIS) server and used widely available tools to gain root access. The compromised server was then used to access the corporate network. Riptech recommended that vendor patches and service packs be regularly applied as appropriate to reduce the potential for a similar attack.

---

[4] Maxwell Utilities is a pseudonym. The actual name of the company has been changed to preserve confidentiality.

During a review of documentation and network diagrams, Riptech consultants identified an unnecessary firewall "hole" in the internal network architecture. This vulnerability, which resulted from improper configuration of the system to allow more convenient administration, was reported to Maxwell engineers and promptly addressed.

1.6.4 Analysis of IT Security in Pharmaceutical Trials

Pharmaceutical companies invest hundreds of millions of dollars each year developing and testing drugs for introduction to the public. Complex scientific innovations are the basis for countless studies leading to the introduction of a new drug in the marketplace.

The lifecycle of a newly innovated drug includes screening of a potential testing population, drug testing (including such things as dosing, blood screening, urine screening – many of which are bar-coded), recording of adverse affects from the drug, checking the data for errors, preparing reports of results, and performing statistical analysis to determine the final results of the tests. To add more complexity to the pharmaceutical studies, several studies on differing populations must occur to assure that effects of the drugs on people of different ages, gender, and ethnicity are positive.

In this life cycle, the integrity of the studies' data is compromised because multitudes of hands touch the data before a "final" product, called an NDA, can be submitted to the FDA for approval. In addition to the risk of data integrity, pharmaceutical companies also have the risk of having their ideas "pirated" by other companies looking to profit off of someone else's intellectual property.

Because of the extraordinary legal, regulatory and financial exposure of the global pharmaceutical manufacturer to both U.S. and European Union "Security, Access and Control " (SAC) regulations, no component of the global clinical trials application is more important than the security model.

- In the United States, companies spend on average $240 million on clinical trials as a drug passes through the Food and Drug Administration (FDA) for final approval. Pharmaceutical companies have billions of dollars at risk if they cannot correctly match a pharmaceutical product to a target patient population as quickly as possible. Lost earnings and revenue by pharmaceutical companies can also occur when a very small segment of a target patient population experiences side effects from an otherwise effective pharmaceutical.
- Healthcare SAC standards in the U.S. are defined by the interaction of state laws with the Health Insurance Portability and Accountability Act (HIPAA). The Act implies that computerized healthcare information systems must have certain features and functions that address the proposed requirements of HIPAA. These requirements are enterprise-wide – that is, above the level of each individual clinical trial application. These requirements must be satisfied by the pharmaceutical manufacturer at the enterprise level. For example, a single global authentication system for each user should be employed by the pharmaceutical manufacturer for all clinical trial applications that access a central collection of data.

The functions required by clinical trials applications to ensure integrity, security, and reliability of the application and its respective data are listed below. These functions in unison create a secure application supporting privacy and security policies that can be applied to an individual or a single transaction:

- Personal Security, Authentication, Role-based Activity, Context-based Activity, Security Policies, Authorization, Ownership, Integrity, Auditable Activity, Security of Data, Message Integrity

The problems pharmaceutical companies face in light of this idea of a global ICH (International Conference on Harmonization) compliant clinical trial architecture can be categorized as follows:

- Management – Grouping users into roles; establishing unique IDs and passwords for all users within a role; setting security policies based on a user's role; authorizing and creating an audit log as dictated by HIPAA; adherence to security standards set by state/country legal authorities
- Application/Data – Determine what applications/data can be accessed and which transactions executed according to user ID/role; show history of access and modifications according to user ID/role; protection of user's data (including work in progress) until data is ready for "general" access; protection of data integrity from unauthorized access (internal and external), modifications, and other SAC threats (including hackers and viruses)
- Network/Web – Ability to protect network messages, data, and applications while transmitting between clinical trial sites; protect data and applications from outsiders (hackers, viruses, etc.)

The solution to expediting the market launch of new drugs is to replace complex multiple submissions of new drug approval with a single folder submission. A single folder submission will save a significant amount of time and resources which will facilitate the approval and the launch of new drugs. The single folder submission will follow the approved Common Technical Document (CTD) guidelines as well as meet ICH guidelines on efficacy, quality and safety. In addition to the submission's conformance to the CTD and ICH guidelines, the submission must be available online and continuously updated.

The technologies that would best support the single folder submission includes "global telecommunications infrastructure, high reliability databases and pervasive access to real-time clinical and ICH dossier data" made up of "best of breed" components. The EMC "E-Infostructure" is the recommended model architecture. Such an architecture combines physical, functional, connectivity, and security layers of hardware and software. The Enterprise Storage Network, ESN, and the Database Management System(s) will make up the storage management layer and will be used to store all information pertaining to the single folder submissions. Oracle Parallel Server or IBM DB2 will support databases for the central repository. Computational, analytical and application-oriented servers which will be used for analyzing information will be made up of highly scalable central processors with high-availability operating systems. Secondary applications will be supported by processors such as Intel-based processors.

As for connectivity, the enterprise storage management software and EMC Symmetrix will integrate all operating systems and database storage into a uniform central repository. The ESN will also serve as the connectivity layer. It will use the information connections, Connectrix and Celerra to connect multiple primary and secondary operating systems to enterprise application and data management platforms. Devices such as a mainframe or a PDA will be able to obtain information through wide and local area access as well as wireless access. TimeFinder will refresh the data warehouse without disruption, and EMC's SRDF can protect clinical trial and other critical data to

prevent any delay in speed to market; it can also be used for disaster recovery and information mobility. There is continuous and secure availability of reporting, decision support, web access and availability of the databases. Each of these capabilities can be replicated to enhance reliability and availability of the operational systems.

1.7 Chapter Summary

Well thought-out security solutions are needed to protect the corporate IT assets that are the backbone of modern digital enterprises. The solutions must employ the latest security technologies to respond to external factors and organizational requirements. This chapter has introduced basic security terms and views and given an overview of the main building blocks of a security solution. The need for a management approach was emphasized, and the idea of viewing security in terms of PIA4 (privacy, integrity, authentication, authorization, accountability, availability) was introduced. A wide range of security technologies, ranging from public/private key encryptions to digital certificates and ACLs, are currently available to address the PIA4 aspects of security. However, IT assets need to be protected at different levels by using approaches and technologies that compensate for and complement each other. An overall solution has been reviewed briefly and a few case studies introduced for illustrative purposes.

Selected Computer Security Books (My Favorites)

Andress, M., *Surviving Security*, SAMS, 2002

Gollman, D., *Computer Security*, Wiley, 1999.

Oppliger, R., *Security Technologies for the World Wide Web*, Artech, 2000.

Pipkin, D., *Information Security: Protecting the Global Enterprise,* Prentice Hall, 2000

Tipton, H. and Kraus, M. (Eds.), *Information Security Management Handbook*, 4th and 5th ed., Auerbach, 2000.

Schneier, B., *Secrets and Lies : Digital Security in a Networked World,* by John Wiley and Sons, 2004.

Stallings, W., *Network Security Essentials*, Prentice Hall, 2000.

Stein, L., *Web Security: A Step-by-Step Reference Guide*, Addison Wesley, 1998.

1.8 Continuing Case Study: Security for Nervous Wreck, Inc. (NRW)

We will use a single case study throughout this book to illustrate how security solutions can be built by using a systematic approach. The case study is based on a fictitious investment company, which we will call Nervous Wreck, Inc. (NRW). This case study is based on a combination of two actual companies. NRW wants its customers to access and update their account information and use some of the firm's financial analysis tools via the Internet. A conceptual model of NRW is shown in Figure 1-9. The NRW corporate website consists of a user interface that connects to an Accounts Balance Program (ABP) that allows customers to view, update, and modify account information; a customer database that contains information about customers; an investment database that contains investment data; and other typical corporate applications and databases for payroll, accounts payable/receivable, etc. A corporate network will operate in the building, connected to the public Internet. A firewall protects the internal corporate resources.

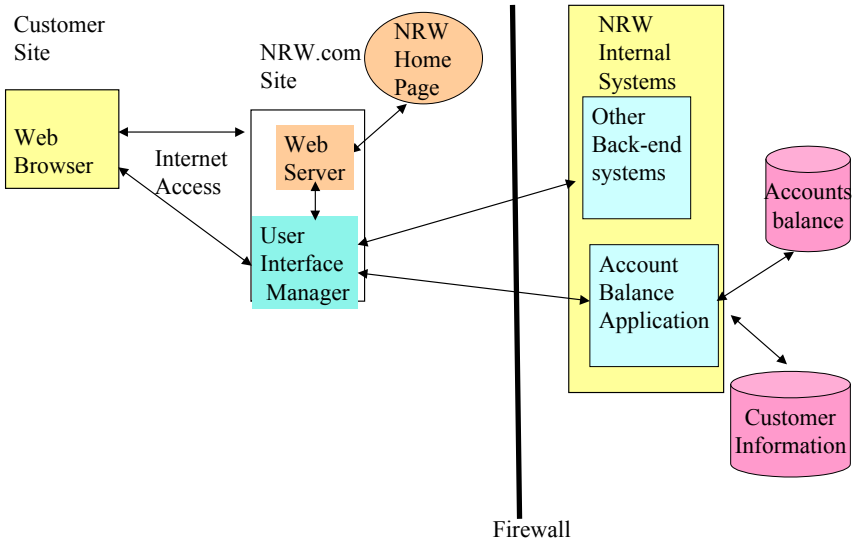


Figure 1-9: NRW System Conceptual View

We will use this case study to lead us through various decisions at the end of each part of the book. Specifically, the following decisions will be illustrated:

- Analyzing the security requirements and developing a security approach (introduced at the end of part 1, chapter 3).
- Selecting appropriate security technologies (introduced at the end of part 2, chapter 6).
- Protecting the wired and wireless networks (introduced at the end of part 3, chapter 9).
- Protecting the distributed platforms and e-commerce/mobile applications (introduced at the end of part 4, chapter 12).
- Building the security solution (introduced at the end of part 5, chapter 14).

1.9 Suggested Review Questions

1) What are the key ingredients of a security solution? In the discussion in this chapter, are there some pieces missing? What are they and why are they important?

2) Suppose you have been asked to develop a document that describes security solution for a bank. Without the technical details, create the table of contents of this document.

3) Are all aspects of PIA4 always needed? Are there too many "As" in this? Would you ignore some? Under what circumstances, and why?

4) Which security technologies address which aspects of PIA4 threats? Show through a table. (Hint: encryption addresses privacy but not necessarily integrity threats.)

5) Why does a security solution need to address all layers of systems (from networks to applications). Why is it not enough just to secure a network or a database by encryption?