Part I
E-security

Introduction to Part I

In enterprise systems, a security exposure is a form of possible damage in the organization's information and communication systems. Examples of exposures include unauthorized disclosure of information, modification of business or employees' data, and denial of legal access to the information system. A vulnerability is a weakness in the system that might be exploited by an adversary to cause loss or damage. An intruder is an adversary who exploits vulnerabilities, and commits security attacks on the information/production system.

Electronic security (e-security) is an important issue to businesses and governments today. E-security addresses the security of a company, locates its vulnerabilities, and supervises the mechanisms implemented to protect the on-line services provided by the company, in order to keep adversaries (hackers, malicious users, and intruders) from getting into the company's networks, computers, and services. E-service is a very closely related concept to e-privacy and it is sometimes hard to differentiate them from each other. E-privacy issues help tracking users or businesses and what they do on-line to access the enterprise's web sites.

Keeping the company's business secure should be a major priority in any company no matter how small or large is the business of the company, and no matter how open or closed the company network is. For this intent, a security policy should be set up within the company to include issues such as password usage rules, access control, data security mechanisms and business transaction protection. A set of good practices that should be followed by any company includes: (a) keep virus scanning software and reactive tools updated; (b) consider the use of stand-alone computers (i.e., computers that are not connected to the network) for sensitive data; (c) define appropriate trusted domains based on the organization of the business activity; (d) install malicious activity detection systems in conformance with the security policy; and (e) define a strong practice of e-mails management (particularly when they are issued from unknown sources and receiving files with known extensions).

E-security solutions aim to provide five important services. These services are: authentication of users and actors, integrity, confidentiality of communication, availability of business services, and non-repudiation of transactions. Most e-security solutions that are

provided by the literature use two main cryptographic techniques: public key cryptosystems and digital signatures. Efficient solutions also should be compliant with the national legal framework, if any.

The first part of the book aims at defining the main concepts used in e-security. It also describes the major techniques and challenging issues in a company's security system. It classifies security attacks and security services and develops the main issues. This part contains three chapters.

Chapter 1 describes the importance of e-security and presents some relevant concepts in network security and subscribers' protection. It also introduces some basic terminology that is used throughout the book to define service, information, computer security, and network security. This chapter aims to provide self-contained features for this book.

Chapter 2 discusses encryption and its practical applications. It focuses on the techniques used in public key cryptosystems. It also details various types of ciphers and their applications to provide the basic e-service solutions. It provides the reader with simple examples that explain how the main concepts and procedures work.

Chapter 3 covers the authentication of users and messages. It details the main schemes of digital signature and their applications. It also addresses the notions of hash function and key establishment. These notions are important because they constitute the hidden part of any protection process that uses public key-based systems.

1 Introduction to e-security

This chapter discusses the importance and role of e-security in business environments and networked systems. It presents some relevant concepts in network security and subscribers protection. It also introduces some basic terminology that is used throughout the book to define service, information, computer security, and network security. This chapter aims at providing self contained features to this book.

1.1 Introduction

Every organization, using networked computers and deploying an information system to perform its activity, faces the threat of hacking from individuals within the organization and from its outside. Employees (and former employees) with malicious intent can represent a threat to the organization's information system, its production system, and its communication networks. At the same time, reported attacks start to illustrate how pervasive the threats from outside hackers have become. Without proper and efficient protection, any part of any network can be prone to attacks or unauthorized activity. Routers, switches, and hosts can all be violated by professional hackers, company's competitors, or even internal employees. In fact, according to various studies, more than half of all network attacks are committed internally.

One may consider that the most reliable solution to ensure the protection of organizations' information systems is to refrain from connecting them to communication networks and keep them in secured locations. Such a solution could be an appropriate measure for highly sensitive systems. But it does not seem to be a very practical solution, since information systems are really useful for the organization's activity when they are connected to the network and legitimately accessed. Moreover, in today's competitive world, it is essential to do business electronically and be interconnected with the Internet. Being present on the Internet is a basic requirement for success.

Organizations face three types of economic impact as possible results of malicious attacks targeting them: the immediate, short-term, and midterm economic impacts. The immediate economic impact is the cost of repairing, modifying, or replacing systems (when needed) and the immediate losses due to disruption of business operations, transactions, and cash flows. Short-term economic impact is the cost on an organization, which includes the loss of contractual relationships or existing customers because of the inability to deliver products

or services as well as the negative impact on the reputation of the organization. Long-term economic impact is induced by the decline in an organization's market appraisal.

During the last decade, enterprises, administrations, and other business structures have spent billions of dollars on expenditures related to network security, information protection, and loss of assets due to hackers' attacks. The rate at which these organizations are expending funds seems to be impressively increasing. This requires the business structures to build and plan efficient strategies to address these issues in a cost-effective manner. They also need to spend large amounts of money for security awareness and employees' training (Obaidat, 1993a; Obaidat, 1993b; Obaidat, 1994).

1.2 Security costs

Network attacks may cause organizations hours and days of system downtime and serious violations in data confidentiality, resource integrity, and client/employee privacy. Depending on the level of the attack and the type of information that has been compromised, the consequences of network attacks vary in degree from simple annoyance and inconvenience to complete devastation. The cost of recovery from attacks can range from hundreds to millions of dollars. Various studies including a long-running annual survey conducted by the Federal Bureau of Investigation (FBI, Los Angeles), and the American Computer Security Institute (CSI) have highlighted some interesting numbers related to these costs. The Australian computer crime and security survey has found similar findings (Gordon *et al*., 2004; Aust, 2004). The surveys have mainly determined the expenditures from a large number of responses collected from individuals operating in the computer and network security of business organizations. The findings of the surveys are described in the following subsections to highlight the importance of security in business structures.

1.2.1 The CSI/FBI computer crime and security survey

Based on responses collected from about 500 information security practitioners in US enterprises, financial institutions, governmental agencies, university centres, and medical institutions, the conclusions of the *2005 Computer Crime and Security Survey* confirmed that the threat from computer hacking and other information security breaches continues to damage the information systems and resources in the surveyed organizations. It also confirmed that the financial cost of the privilege of using the information technologies is increasing for the tenth year. It reports also that, except for the abuse of wireless networks, all the categories of attacks of information systems have been slowly decreasing over many years. Major highlights of the *Survey* include:

- Virus attacks and denial of service attacks continue to be the major source of financial losses, while unauthorized accesses show an important cost increase.
- Over 87% of the surveyed organizations have conducted security audits during 2005 to assess the efficiency of their security solutions. Only 82% had conducted security audits in 2004.

- The majority of the organizations did not outsource system security activities.
- The average reported computer security operating system and investment per employee was high for firms with low annual sales and decreased for companies with very high annual sales.
- The large majority of the organizations have considered security awareness and training as an important task, although (on average) respondents from all sectors have declared that they do not believe that their organization invests enough in this area.

The survey has identified four areas of interest to measure the importance of security issues in conducting business and competing with other organizations. These areas are: (a) budgeting, (b) nature and cost of cyber-security breaches, (c) security audits and security awareness, and (d) information sharing. The overall findings of the survey can be summarized by the following issues:

Budgeting issues

These issues consider the costs associated with security breaches, financial aspects of information security management, and solutions implementation. Two major indicators have been considered. They are: (a) the percentage of the information security budget relative to the organization's overall IT budget and (b) the average computer security operating expense and investment per employee.

The 2004 survey has reported that 5.46% of the respondents have indicated that their organizations allocated between 1% and 5% of the total IT budget to security, while only 16% of the respondents have indicated that security received less than 1% of the IT budget. Moreover, 23% of respondents indicated that security received more than 5% of the budget, however, 14% of respondents indicated that the portion was unknown to them. The results of the survey also demonstrate that as an organization grows, computer security operating and capital expenditures grow less rapidly. This highlights the fact that there is economy of scale when it comes to information security.

On the other hand, the 2005 survey has shown another tendency. Firms with annual sales under $10 million spent an average of $643 per employee on operating expenses and investment in computer security. The largest firms have only spent an average of $325 per employee.

Spending per employee on information security, broken down by sector, shows a slightly different scenario compared to the results provided in the 2004 survey. The highest average computer security spending was reported by state governments. The next highest sectors are utilities, transportation, and telecommunications. The highest sectors reported in the 2004 survey were transportation, Federal government, and telecommunications. Two observations should be mentioned, however:

1. Securing state governments is a very hot issue nowadays.
2. Managers responsible for computer security are increasingly asked to justify their budget requests in economic terms (ROI, for example).

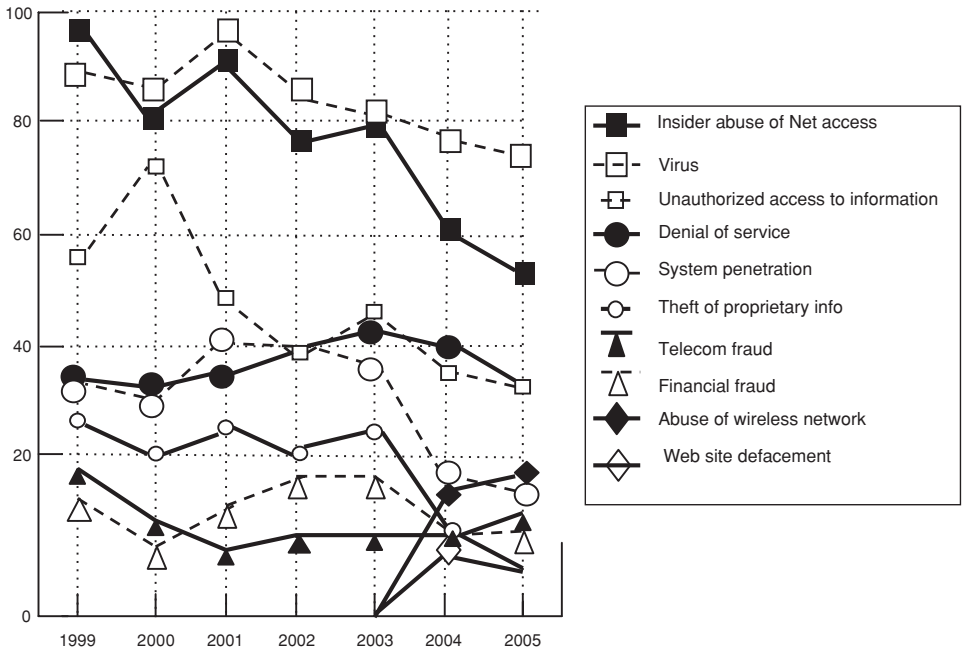

Figure 1.1 Types of attacks reported for 2005 (BFI/CSI 2005 survey).

Nature of attacks

Figure 1.1 depicts the percentage of respondents detecting attacks per type of attack. It shows that detected attacks and misuses have been slowly decreasing over the last years. Two categories, however, have shown an important increase: Web site defacement and the abuse of wireless networks.

The 2004 survey demonstrates that the denial of service category of attacks has emerged for the first time as the incident type generating the largest total losses (replacing theft of proprietary information, which had been the most expensive category of loss for the five previous years). It has shown also that the respondents have reported abuse of wireless networks (15% of the respondents), Web site defacement (7%) and misuse of public Web applications (10%).

The 2005 survey reports that the total losses were dramatically decreasing. But, beyond the overall decline, viruses, unauthorized accesses, and denial of services are generating 61% of financial losses. In addition, two areas of increase can be noticed, unauthorized access to information, where the average loss per respondent moved up from $51 000 to $300 000, and theft, where the average loss moved from $168 000 to $355 000.

Security audits and awareness

The 2004 survey found that 82% of respondents indicated that their organizations conducted security audits. This percentage has increased to 87% in the 2005 survey. In addition to

security audits the surveys demonstrate that investing in security learning did not reach an acceptable level since on average, respondents from all sectors reported in the 2004 and 2005 surveys do not believe their organizations invest enough in security awareness. Respondents also share the following thoughts:

1. Security awareness training was perceived most valuable in the areas of security policy and security management (70%), followed by access control systems (64%), network security (63%), and cryptography (51%).
2. The two areas in which security awareness was perceived to be the least valuable were: security systems architecture, and investigations and legal issues.

Information sharing

The 2004 survey shows that only half of all respondents indicated that their organizations share information about security breaches and that more than 90% of respondents indicated that their organization responds by patching security holes. However, 57% of the respondents indicated that their organization does not belong to any incident/response information-sharing organization. Over 50% of respondents (among those indicating that their organization would not report an intrusion to law enforcement agencies) declared as very important the perception that the negative publicity would hurt their organization's stock and/or image. The findings of the 2005 survey are similar. This latter survey has shown that 46% of the respondents indicated that their organization does not belong to any information-sharing group.

1.2.2 *The Australian computer crime and security survey*

The Australian *Computer Crime and Security Survey* provides a unique insight into the information security operations of Australian organizations ranging from single person enterprises to large corporations. The results of the 2005 survey presents some similarities with the results reported by the *2004 Computer Crime and Security Survey* (Gordon *et al*., 2004) and show the following key findings:

1. More respondent organizations have experienced electronic attacks that harmed the confidentiality, integrity, or availability of network data or systems compared to the previous year.
2. Infections from viruses, worms or Trojans were the most common form of electronic attacks reported by respondents for the consecutive year. They were the greatest cause of financial losses and accounted for 45% of total losses for 2004. However, denial of service attacks that have been reported by the 2005 survey were the greatest cause of financial losses.
3. The readiness of organizations to protect their IT systems has improved in three major areas: (a) the use of information security policies, practices, and procedures; (b) the use of information security standards; and (c) the number of organizations with experienced, trained, qualified or certified staff.

4. Unprotected software vulnerabilities and inadequate staff training and education in security practices were identified as the two most common factors which contributed to harmful electronic attacks.
5. The most common challenges and difficulties that respondent organizations faced were changing user attitudes and behavior and keeping up to date with information about the latest computer threats and vulnerabilities.

Therefore, the effort being made by responding organizations to improve their readiness to protect their systems appeared to be insufficient to cope with the changing nature of the threats and vulnerabilities. This includes the increased number and severity of system vulnerabilities as well as the growing number and rapid propagation of Internet worms and viruses.

Nature and impact of electronic attacks

The survey shows that 95% of respondents have experienced one or more security attacks, computer crime, computer access misuse, and abuse in the last 12 months. The most common incidents were virus, worm and Trojan infections (88% in 2004, compared to 80% in 2003 and 76% in 2002); insider abuse of Internet access, email or computer system resources (69% in 2004, compared to 62% in 2003 and 80% in 2002); and laptop theft (reported 58% in 2004, compared to 53% in 2003 and 74% in 2002).

Impact can be measured in direct and indirect costs, time to recover, and intangible impacts such as damage to an organization's credibility, trustworthiness, or reputation. The impact of electronic attacks, computer crime and computer access misuse ranges from negligible to grave, in both cost and time. Overall, the losses experienced by respondent organizations as a whole have got worse (20% higher than in 2003) with average of $116 212 for each organization that quantified its losses. By comparison, in 2003 the average loss was $93 657 and in 2002 it was $77 084.

The cost of computer crime

The survey ranges the cost based on a set of sixteen causes of loss that were incurred including: (a) virus, worm, and Trojan infections (54% of the total losses); (b) computer facilitated financial fraud (15% of the total losses); (c) degradation of network performance (11% of the total loss); (d) laptop theft; and (e) theft/violation of proprietary or confidential information. The survey, however, demonstrates that sabotage of data or communication networks, telecommunications fraud, denial of service attacks, system penetration by outsiders, and unauthorized access to information by insiders do not exceed 9% of the total annual losses.

For the vast majority of electronic attacks, computer crimes, computer access misuse incidents, recovery time was between one to seven days or less than a day. For respondents that estimated the time it took to recover from the most serious incident they had in each of the sixteen listed categories, 60% estimated that they recovered in less than a day; 74% estimated that recovery took between one to seven days; 28% estimated that recovery took

between eight days to four weeks; 13% estimated that recovery took more than one month; and 5% experienced incidents which they assessed they may never recover from.

1.3 Security services

Information and network security risks are increasing tremendously with the growth of the number of threats and the sophistication of attacks. To cope with this growth, incidents of viruses, hackers, theft, and sabotage are being publicized more frequently and the enterprise management has started keeping an interest on the archives developed. A non-exhaustive list of simple security incidents contains, but is not limited to, the following examples of security breaches (Stallings, 2001):

- A user, named Us_A, transmits a file to another user named Us_B. The file containing sensitive information (e.g., financial transaction and private data) should be protected from disclosure. User Us_H, who is not authorized to access the file content, is able to capture a copy of the file during its transmission on the network, if the file is not well protected.
- A network manager, named Man_D, transmits a message to a networked computer, called Com_E, to update an authorization file and include the identities of new users who are to be granted access to Com_E. User Us_H, who is an adversary, intercepts the message, alters its content, and forwards it to Com_E. Computer Com_E accepts the message as coming from Man_D and updates its authorizations accordingly.
- A message is sent from a customer Us_A to a stockbroker Us_B with instructions to execute various transactions. User Us_H may intercept the message and get a copy of it. Subsequently, Us_H sends several copies of the message inducing a multiple execution of the initial transaction, generating by this way financial losses to Us_A.
- An employee is discharged without warning. The personnel manager sends a message to a server system to invalidate the employee's account. When the invalidation is accomplished, the server posts a notice to the employee's file as confirmation of the action. The employee is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information.

As information systems become essential to conduct business, electronic information takes care of many of the roles traditionally performed by paper documents. According to this consideration, functions that are traditionally associated with paper documents must be performed on documents that exist in electronic form. To assess effectively the security needs of an organization and evaluate or select security products and policies, the manager responsible for the organization's security may need a systematic way of defining the requirements for security and characterizing the approaches to satisfy those requirements. For this, three aspects of information security need to be considered:

- **Security attacks** A security attack is defined to be any action that compromises (or attempts to compromise) the security of the information system (or information resources) owned by an organization, an employee, or a customer.

- **Security mechanisms** These are mechanisms (procedures, applications, or devices) that are designed to detect, prevent, or recover from security attacks.
- **Security services** These are services that enhance the security of the data processing and the information transfers of an organization. The services are intended to counter security attacks and assumed to make use of one or more security mechanisms.

1.3.1 *Security services*

Several aspects of electronic documents make the provision of security functions or services challenging (Stallings, 2001). These services include but are not limited to the following:

Authentication

The authentication service aims at assuring that a communication is authentic (genuine). This requires that the origin of a message must be correctly identified, with assurance that the identity is not false. In the case of a single message, the authentication service assures the recipient that the message is issued from the source that it claims to be from. In the case of an ongoing interaction, two aspects are involved. First, at the time of connection establishment, the service assures that the two communicating entities are authentic. That is, each entity has the identity that it claims to have. Second, the service assures that the connection is not interfered with by another connection in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception of sensitive information.

Confidentiality

This service requires that the information in a computer system, as well as the transmitted information, be accessible only for reading by authorized parties. Therefore, confidentiality is the protection of static and flowing data from attacks. It is also related to the protection of information from unauthorized access, regardless of where the information is located, how it is stored, or in which form it is transmitted. Several levels of protection can be identified and implemented to guarantee such service. The broadest service protects all user data transmitted between two users over a period of time. Limited forms of the confidentiality service can address the protection of a single message or even specific fields within the message.

Integrity

This service ensures that computer systems resources and flowing information can only be modified by authorized parties. Integrity is the protection of information, applications, systems, and networks from intentional, unauthorized, or accidental changes. It can apply to a stream of messages, a single message, or specific parts of a message. Two classes of integrity services can be considered: connection-oriented integrity and connectionless integrity. A connection-oriented integrity service guarantees that messages in a given connection are