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).

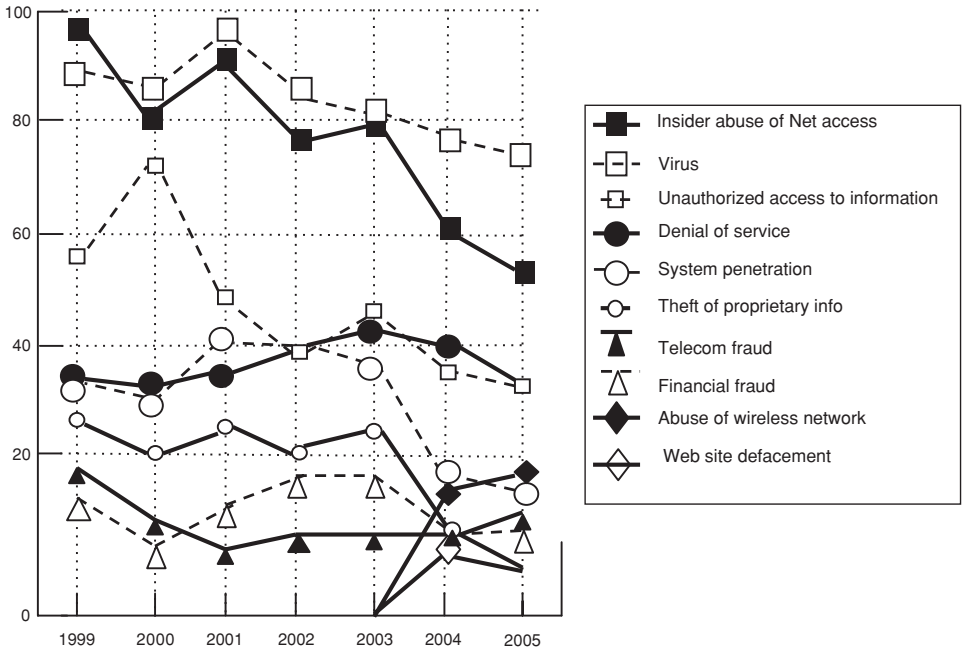

Figure 1.1 Types of attacks reported for 2005 (BFI/CSI 2005 survey).

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

received as sent, with no duplication, insertion, modification, reordering, or replay. The delete/destruction of data is also controlled by this service. On the other hand, a connectionless integrity service deals with individual messages and typically provides protection against message modification only.

Non-repudiation

This service guarantees that neither the sender of a message can deny the transmission of the message nor the receiver of a message is able to deny the reception of the message. Therefore, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can prove that the message was in fact received by the legitimate receiver. The technical control used to protect against non-repudiation can be provided by the so-called digital signature.

Access control

This service guarantees that access to information be controlled by (or on behalf of) the target system. In the context of network security, access control is the ability to limit and control the access to host systems and applications via communication links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individuals. Access control protects against unauthorized use or manipulation of resources through authentication and authorization capabilities. Authorization services ensure that access to information and processing resources is restricted based on the management of a security policy.

Availability function

This is the property of a system, network, or a resource being accessible and usable any time upon demand by an authorized system entity, according to performance specifications for the system. This means that a system is available if it provides services according to the system design whenever users require them. The X.800 standard considers availability as a property to be associated with various security services such as services protecting from denial of service.

1.3.2 Security attacks

Security attacks include interruption (i.e., an asset is destroyed or becomes unavailable), interception (this happens when an unauthorized party gains access to an asset), modification, and fabrication (particularly visible when an unauthorized party inserts counterfeit objects such as messages or files). A primary way to classify security attacks considers that attacks can be either passive or active. Passive attacks aim to gain information that is being transmitted. Passive attacks are very difficult to detect because they do not involve any alteration of the observed data or the network resources. However, it is feasible to prevent the success of these attacks, usually by means of encryption for example. A particular

example of passive attacks of some importance is the traffic analysis attack, which permits the intruder to observe communications and learn about transmission time, size, and structure of transmitted messages. They allow getting copy of the exchanged data and using it to extract confidential information. They also determine the location and the identity of communicating hosts (e.g., service location, used ports, and IP addresses).

Active attacks involve some modification of the data flow, to be attacked, or the creation of a false data stream. They can be subdivided into different categories: impersonate attacks, replay, modification, and denial of service. An impersonate attack takes place when an entity pretends to be a different entity in order to obtain extra privileges. It usually includes one of the forms of active attacks. A valid authentication message can be captured and resent to gain specific interest. A replay attack involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect. A modification means that some portion of a legitimate message (or a file) is altered, delayed or reordered to produce unauthorized effects. Examples of modifications include modifying routing tables within a network router and modifying the content of transactions.

A denial of service prevents or reduces the normal use, operation, or management of communication facilities. Denial of service attacks attempt to block or disable access to resources at the victim system. These resources can be network bandwidth, computing power, buffers, or system data structures. The different categories of denial of service attacks can be mainly classified into software exploits and flooding attacks. In software exploits, the attacker sends a few packets to exercise specific software bugs within the target service or application, disabling the victim. In flooding attacks, one or more attackers can send continuous streams of packets for the purpose of overwhelming a communication protocol or computing resources at the target system.

Based on the location or observation points, attacks can be classified as single-source when a single zombie (i.e., procedure that acts on behalf of the attacker) is observed performing the attack to the targeted victim, and as direct multi-source when multiple distributed zombies are attacking the victim system. Often, zombies are typically injected procedures or insecure objects that have been compromised by a malicious user.

1.4 Threats and vulnerabilities

In this section, we consider the notion of vulnerabilities noticeable on each asset within an enterprise information and communication system. We will also consider threats to hardware, applications, and information. Since physical devices are so visible, they are rather simple targets to attack. Serious physical attacks include machine-slaughter, in which an adversary actually intends to harm an information system. Fortunately, however, reasonable safeguards can be put down to protect physical assets (West-Brown *et al.*, 1998; Allen, 2001).

A secure processing environment within an organization includes making sure that only those who are authorized are allowed to have access to sensitive information, that the information is processed correctly and securely, and that the processing is available when

necessary. To apply appropriate security controls to an operating environment, it is necessary to understand who or what poses a threat to the operating environment; and therefore to understand the risk or danger that the threat can cause. When the risk is assessed, management procedures must decide how to mitigate the risk to an acceptable level. Another approach for managing security controls resides in providing some degree of compensation for losses/damages by contracting insurance.

Vulnerabilities, threats, and risks are defined in what follows. They will be studied to a large extent in Chapter 14 where the risk management is completely addressed.

Vulnerabilities

A security vulnerability is a weakness (e.g., a flaw or a hole) in an application, product, or asset that makes it infeasible to prevent an attacker from gaining privileges on the organization's system, compromising data on it, modifying its operation, or assuming non-granted trust. The following simple examples would constitute security violations:

- A flaw in a web server that enables a visitor to read a file that he/she is authorized to read.
- A flaw that allows an unauthorized user to read another user's files, regardless of the permissions on the files.
- The fact that an attacker could send a large number of legitimate requests to a server and cause it to fail.
- A flaw in a payment gateway allowing price manipulation to be transmitted unnoticed.

Threats

An organization's information can be accessed, copied, modified, compromised, or destroyed by three types of threats: intentional, unintentional, or natural threats. Intentional threats are unauthorized users who inappropriately access data and information that they are not granted privilege to read, write, or use. These users can be external or internal to the organization and can be classified as malicious. The malicious users have intent to steal, compromise, or destroy assets. Intrusion by malicious unauthorized users first attempts to get results in a breach of confidentiality and second by causing breaches in integrity and availability.

Unintentional threats are typically caused by careless or untrained employees who have not taken the steps to ensure that their privileges are protected, their computers are properly secured, or that virus scanning software is frequently updated. Unintentional threats also include programmers or data processing personnel who do not follow established policies or procedures designed to build controls into the operating environment. Unintentional threats can affect the integrity of the entire application and any integrated applications using common information.

Natural threats include, but are not restricted to, equipment failures or natural disasters such as fire, floods, and earthquakes that can result in the loss of equipment and data. Natural threats usually affect the availability of processing resources and information.

Risks

There are many events that can be generated if a breach of confidentiality, integrity, or unavailability occurs. From the business point of view, there is always financial loss involved. The business risks include contractual liability, financial misstatement, increased costs, loss of assets, lost business, and public embarrassment. Increased costs occur from many types of security incidences. A lack of integrity in systems and data will result in significant cost to find the problem and fix it. This could be caused by the modification, testing, and installation of new programs and rebuilding systems.

Controls

Controls fall into three major categories: physical, administrative, and technical. Physical controls constrain direct physical access to equipment. They consist of cipher locks, keyboard locks, security guards, alarms, and environmental systems for water, fire, and smoke detection. Physical controls also consist of system backups and backup power such as batteries and uninterruptible power supply.

Administrative controls include the enforcement of security policies and procedures. Policies inform users on what they can and cannot do while they use the organization's computing resources. Procedures help the management review the changes to code, authorization for access to resources, and periodic analysis. They tell how to check that an access is still appropriate, perform separation of tasks, realize security awareness, and plan for technical training. Administrative controls can be continuous, periodic, or infrequent. They contain documents on IT management and supervision, disaster recovery, and contingency plans. Administrative controls also include security review and audit reporting that are used to identify if users are adhering to security policies and procedures. Technical controls are implemented through hardware or software, which typically work without human intervention. They are usually referred to as logical controls. Specific software controls include anti-virus, digital signatures, encryption, dial-up access control, callback systems, audit trails, and intrusion detection systems.

Administrative, technical, and physical controls can be further subdivided into two categories: preventive or detective. Preventive controls, such as technical training, attempt to avoid the occurrence of unwanted events, whereas detective controls, such as security reviews and audits, attempt to identify unwanted events after they happen. When an event does occur, controls involving the detection and analysis of related objects are designed to catch the problem quickly enough to minimize the damage and be able to accurately assess the magnitude of the damage caused.

1.5 Basics of protection

Security solutions attempt to establish perimeters of protection (for security domains) to filter the entering and the available data. A security solution depends on the correctness and the reliability of three related components: security policy, implementation mechanisms,

and assurance measures. In the following, we attempt to characterize the notions of security domain and security policy in an enterprise, and show how they are related to each other.

1.5.1 Security management

Security policies set the guidelines for operational procedures and security techniques that reduce security risks with controls and protective measures. A security policy has a direct impact on the rules and policing actions that ensure proper operation of the implemented mechanisms. Policy has an indirect influence on users; they see security applications and access services, not policies. The security policy of an organization should also determine the balance between users' ease of use and the level of responsibility. The amounts of controls and countermeasures should also be considered.

The goal of a security manager is to apply and enforce consistent security policies across system boundaries and throughout the organization. The challenges in achieving a functional security system include two constraints. First, a consistent and complete specification of the desired security policy needs to be defined independently of the implementing technologies. Second, satisfying the need for a unified scheme to enforce the applicable security policies using and reusing available tools, procedures, and mechanisms. The difficult task in achieving an acceptable *state of security* is not obtaining the necessary tools, but choosing and integrating the right tools to provide a comprehensive and trustworthy environment.

Security management can be defined as the real-time monitoring and control of active security applications that implement one or more security services in order to keep the organization's system at an acceptable state of security. The purpose of security management is to ensure that the security measures are operational and compliant with the security policy established by the organization. Not only must the security services function correctly, but they must counteract existing threats to generate justifiable confidence in the system trustworthiness.

Network security management is by nature a distributed function. Applications that may be under the coverage of security management include firewalls, intrusion detection systems, and security control applications. Security management faces the same security threats that other distributed applications have to face. Coordinated management of security is not feasible without a secure management infrastructure that protects the exchanged messages from blocking, modification, spoofing, and replay. Although the discussion of security management architecture is beyond the scope of this section, it is obvious that management, access control, and reliable implementation of management software are also critical.

In its simplest form, security management could require the presence of skilled employees at each security device. It also requires manual evaluation of all significant events. On the other hand, security experts do believe that remote monitoring with computer-assisted correlation of alerts and management of system events is just as efficient for security management as it is for network management. In fact, it may be argued that detection of sophisticated attacks needs the help of sophisticated decision-support systems. In its more

advanced form, security management should integrate what is called security assurance and rely on the notion of trust domain.

Assurance is the conventional term for methods that are applied to assess and ensure a security system enforces and complies with intended security policies. One may use assurance tools before, during, or after security mechanism operations. A trusted domain comprises systems (and network components) or parts of systems (e.g. security modules, computers, and routers), with the assumption that no attackers are assumed within a trusted domain. This restriction induces the fact that a trusted domain is always related to a single user or group of users accessing specific applications.

1.5.2 Security policies

Defining a Security Policy (SP) has been the subject of a big debate in the security community. Indeed, although this concept has been addressed by many specialists, it turns out to be hard to find a definition that relates a uniform view. In Hare (2000), SP has been presented as a "*high level statement that reflects organization's belief related to information security*." We believe that an information security policy is designed to inform all employees operating within an organization about how they should behave related to a specific topic, how the executive management of the organization should behave about that topic, and what specific actions the organization is prepared to take. Security policy should specify the policy scope, responsibilities, and management's intention for implementing it. It addresses security activities that include designing controls into applications, conducting investigation of computer crimes, and disciplining employees for security violation. Security policies also include standards, procedures, and documents.

Standards constitute a specific set of rules, procedures or conventions that are agreed upon between parties in order to operate more uniformly, effectively, and regardless of technologies. Standards have a large impact on the implementation of security. When they are taken into consideration, they can impact the amount of support required to meet the enterprise security objectives. This will have a definite impact on both cost and the level of security risk. Procedures are plans, processes, or operations that address the conditions of how to go about a particular action.

The constituency of the SP is also a fundamental issue that is tightly related to both objectives and requirements. The major components of a good SP should include (IETF, 1997):

1. An *Access Policy* which defines privileges that are granted to system users in order to protect assets from loss or misuse. It should specify guidelines for external connections and adding new devices or software components to the information system.
2. An *Accountability Policy* that defines the responsibilities of users, operations staff, and management. It should specify the audit coverage and operations and the incident handling guidelines.
3. An *Authentication Policy* which addresses different authentication issues such as the use of Operating System (OS) passwords, authentication devices or digital certificates. It should provide guidelines for use of remote authentication and authentication devices.

4. An *Availability Policy*, which defines a set of user's expectations for the availability of resources. It should describe recovery issues and redundancy of operations during down time periods.
5. A *Maintenance Policy*, which describes how the maintenance people are allowed to handle the information system and network. It should specify how remote maintenance can be performed, if any.
6. A *Violations Reporting Policy*, which describes all types of violations that must be reported and how reports are handled.
7. A *Privacy Policy*, which defines the barrier that separates the security objectives from the privacy requirements. Ideally, this barrier must not be crossed in both directions.
8. A set of *supporting information*, which provides systems users and managers with useful information for each type of policy violation.

Generally, the most important goals that might be achieved by a security policy are described through the three following points:

1. The measures of the SP should maintain the security of critical components at an acceptable level. In other terms, the security policy helps enterprises in reducing the likelihood of harmful adverse events.
2. The security policy must include some response schemes that make the system recover if an incident (e.g., security attack, or natural disaster) occurs.
3. The security policy must ensure the continuity of the critical processes conducted by an enterprise whenever an incident occurs.

Achieving these objectives requires a solid interaction between the security policy and the remaining strategic documents of the organization such as the Disaster Recovery Plan (DRP), the Incident Response Plan (IRP), and the Business Continuity Plan (BCP).

To develop security policies and procedures, one must undertake the following activities: (a) look at what the organization desires to protect, by taking an inventory of all applications, operating systems, databases, and communication networks that compose the organization's information system; (b) determine who is responsible for these components; (c) look with the resource owners at the resource from a confidentiality, integrity, and availability point of view; and (d) determine how to protect the resource in a cost-effective manner based on its value to the enterprise.

Threat and realistic risk estimation are necessary components of this activity. Security baseline of risk estimation is typically an important step to be performed because of security audit requirements and the need to classify the state of security of a system. Policies, standards, and procedures should be reviewed continuously and improved every time a weakness is found. Risk estimation should also be a continuous process because of two facts: (a) the distributed organization's computing environment is always changing and (b) threats and attacks are increasing in number, complexity, and ability to create damage.

Particular policies that relate to protection are the e-mail policy, Internet policy, and e-commerce policy. The e-mail policy is designed to protect business partners' interest, client information, the employee, and the enterprise from liability. The e-mail security policy covers several subjects including the confidentiality and privacy of mails, passwords,

and mail servers. It also discusses how to protect sensitive information through the use of encryption, the limits of personal use of the e-mail system, procedure for communicating with individuals outside the enterprise, and restriction related to communications or information provided to corporate entities, business partners, or customers.

In addition to e-mail, and other Internet services such as the transfer of files (FTP), the ability to log on remotely to a host at another location (Telnet), web service discovery and brokering are used. Such services show the necessity to establish an Internet security policy since there are significant risks related to providing a network connection from the internal network of the enterprise to the Internet. The major risks include the destruction, downtime, and maintenance costs dues to viruses, potential access to internal information, and vulnerabilities from competent, and technically proficient yet destructive hackers.

1.6 Protections of users and networks

1.6.1 Protection of employees

Protection of users includes the following major tools: the shared key encryption schemes, crypto-hash functions, the public key encryption schemes and the digital signature schemes.

Shared key encryption schemes

In its simplest terms, encryption is the process of making information and messages flowing through the network unreadable by unauthorized individuals and entities. The process may be manual, mechanical, or electronic. We, however, consider that the encryption systems in this book are only electronic and are achieved through well-established standards. The conceptual model of an encryption model consists of a sender and a receiver, a message (called the *plain text*), the encrypted message (called the *cipher text*), and an item called secret key. The encryption process (or cryptographic algorithm) transforms the plain text into the cipher text using the key. The key is used to select a specific instance of the encryption process embodied in the transformation.

Examples of encryption algorithms include DES, 3DES, IDEA, AES, (Stallings, 2001). These schemes can handle data messages of several Gigabyte/s and use keys of varying size in the range of 56–128–192–256 bits. Although encryption is an effective solution, its effectiveness is limited by the difficulty in managing encryption keys (i.e., of assigning keys to users and recovering keys if they are lost or forgotten).

Hash functions

A Hash Function H generates a value $H(m)$, for every variable-length message $H(m)$ called the message digest of m. A hash function assumes first that it is easy to compute any message digest, but assumes that it is virtually impossible to generate the message code knowing only its digest. Second, collision resistance is provided; i.e., an alternative message hashing

to the same value cannot be found. This prevents forgery when encrypted hash code is used and guarantees message authentication of the message given its digest.

Digital signature schemes

Digital signature is an electronic process that is analogous to the hand written signature. It is the process of binding some information (e.g., a document or a message) to its originator (e.g., the signer). The essential characteristic of a digital signature is that the signed data unit cannot be created without using a key private to the signer, called *private key*. This means three things:

1. The signed data message cannot be created by any individual other than the holder of the private key used for the signing.
2. The recipient cannot create the signed data unit, but can verify it using the related publicly available information; the public key.
3. The sender cannot deny signing and sending the signed data unit.

Therefore, using only publicly available information, it is possible to identify the signer of a data unit as the possessor of the related private key. It is also possible to prove the identity of the signer of the data unit to a reliable third party in case a dispute arises. A digital signature certifies the integrity of the message content, as well as the identity of the signer. The smallest change in a digitally signed document will cause the digital signature verification process to fail. However, if the signature verification fails, it is in general difficult to determine whether there was an attempted forgery or simply a transmission error.

1.6.2 *Protection of networks*

Various mechanisms are typically used to protect the components of a communication network. They include, but are not limited to, the following mechanisms:

Firewalls

A firewall is a security barrier between two networks that analyzes traffic coming from one network to the other to accept or reject connections and service requests according to a set of rules, which is often part of the overall security policy or separated for updating these rules to cope with the attack growth. If configured properly, a firewall addresses a large number of threats that originate from outside a network without introducing any significant security danger. Firewalls can protect against attacks on network nodes, hosts, and applications. They also provide a central method for administering security on a network and logging incoming and outgoing traffic to allow for accountability of users' actions and for triggering incident response activity if unauthorized activities occur.

Firewalls are typically placed at gateways to networks to create a security perimeter to primarily protect an internal network from threats originating from outside, particularly, from the Internet. However, the most important issue in effectively using firewalls is developing a firewall policy. A firewall policy is a statement of how a firewall should work through a set

of rules by which incoming and outgoing traffic should be authorized or rejected. Therefore, a firewall policy can be considered as the specification document for a security solution that has to protect in a convenient way the organization's resources and processes.

Firewall products have improved considerably over the past several years and are likely to continue to improve. The firewall technology is evolving towards distributed and high-speed organization in order to cope with the growing application needs and sophistication of networks.

Access, authorization, and authentication tools

Access control mechanisms are used to enforce a policy of limiting access to a resource to only authorized users. These techniques include the use of access control lists or matrices, passwords, capabilities, and labels, the possession of which may be used to indicate access rights. Authorization involves a conformance engine to check credentials with respect to a policy in order to allow the execution of specific actions. Authentication attempts to provide a proof of the identity of a user accessing the network (Obaidat, 1997; Obaidat, 1999).

Intrusion detection systems

Intrusion detection is the technique of using automated and intelligent tools to detect intrusion attempts in real-time manner. An *Intrusion Detection System* (IDS) can be considered as a *burglar alarm for computer systems and networks*. Its functional components include an analysis-engine that finds signs of intrusion from the collection of events and a response component that generates reactions based on the outcome of the analysis engine. Chapter 11 will discuss the IDS's concepts, usage, and promises.

Two basic types of intrusion detection systems exist: rule-based systems and adaptive systems. Rule-based systems rely on libraries and databases of known attacks or known signatures. When incoming traffic meets specific criteria, it is labeled as an intrusion attempt. There are two approaches for rule-based IDSs: peremptory and reactionary. In the peremptory approach, the intrusion tool actually listens to the network traffic. When suspicious activity is noted, the system attempts to take the appropriate action. In the reactionary approach, the intrusion detection tool watches the system logs instead, and reacts when suspicious activity is noticed.

Adaptive/reactive systems use more advanced techniques including multi-resolution operational research, decision support systems, and learning processes to achieve its duties.

1.7 Security planning

Security planning begins with risk analysis, which is the process that determines the exposures and their potential harms. Then it lists for all exposures possible controls and their costs. The last step of the analysis is a cost-benefit analysis that aims at answering questions like:

Does it cost less to implement a control or accept the expected cost of the loss?

Risk analysis leads to the development of a security plan, which identifies the responsibilities and the certain actions that would improve system security (Swanson, 1998).

1.7.1 Risk analysis

Risk analysis is concerned with setting up relationships between the main risk attributes: assets, vulnerabilities, threats, and countermeasures. Since the concept of risk is commonly considered as simply part of the cost of doing business, security risks must be taken as a component of normal operation within an enterprise. Risk analysis can reduce the gravity of a threat. For example, an employee can perform an independent backup of files as a defense against the possible failure of a file storage device. Companies involved in extensive distributed computing cannot easily determine the risks and the controls of the computer networks. For this reason, a systematic and organized approach is needed to analyze risks.

For companies, benefits of careful risk analysis include: (a) the identification of assets, vulnerabilities, and controls, since a systematic analysis produces a comprehensive list that may help build a good solution; (b) the development of a basis for security decisions, because some mechanisms cannot be justified only from the perception of the protection they provide; and (c) the estimation/justification for spending on security since it helps to identify instances that justify the cost of a major security mechanism.

Risk analysis is developed extensively in Chapter 14. It is a methodical process adapted from practices in management. The analysis procedure consists of five major steps: (a) assets identification; (b) vulnerabilities determination and likelihood of exploitation estimation; (c) computation of expected annual loss; (d) survey of applicable controls and their costs; and (e) annual savings of control projection. The third step in risk analysis determines how often each exposure will be exploited. Probability of occurrence relates to the severity of the existing controls and the probability that someone or something will elude the existing controls.

Despite its common usage, there are arguments against risk analysis management. First, the lack of precision of risk analysis methods is often mentioned as a deficiency. The values used in the method, the likelihood of occurrence, and the cost per occurrence are not precise. Second, providing numeric estimation may produce a false impression of precision or security. Third, like contingency plans, risk analysis has an inclination to be stored and immediately forgotten.

1.7.2 Security plans

A security plan is a document that describes how an organization will address its security needs. The plan is subject to periodic review and revision as the security needs of the organization change and threats increase. The security plan identifies and organizes the security activities for a networked information system. The plan is both a description of the current situation and a plan for change. Every security plan should be an official documentation of current security practices. It can be used later to measure the effect of the change and suggest further improvements.

A security plan states a policy on security. The policy statement addresses the organization's goals on security (e.g., security services, protection against loss, and measures to protect business from failure), where the responsibility for security lies (e.g., security group, employees, managers), and the organization's commitment to security. The security plan should define the limits of responsibility (such as which assets to protect and where security boundaries are placed). It should present a procedure for addressing a vulnerability that has not been considered. These vulnerabilities can arise from new equipment, new data, new applications, new services, and new business situations.

If the controls are expensive or complicated to implement, they may be acquired from the shelf and implemented gradually. Similarly, procedural controls may require the training of the employees. The plan should specify the order in which the controls are to be implemented so that most serious exposures are covered as soon as possible. A timetable also should be set up to give milestones by which the progress of the security program can be evaluated. An important part of the timetable is establishing a date for evaluation and review of the security solution.

As users, data, and equipment change, new exposures develop and old means of control become obsolete or ineffective. Periodically the inventory of objects and the list of controls should be updated, and the risk analysis should be reviewed. The security plan should set a time for this periodic review. After the plan is written, it must be accepted and its recommendations be carried out. A key to the success of the security plan is management commitment, which is obtained through understanding the cause and the potential effects of security lack, cost effectiveness, and presentation of the plan.

1.8 Legal issues in system security

Law and information systems are related in different manners. First, laws affect privacy and secrecy and typically apply to the rights of individuals to keep personal information private. Second, laws regulate the development, ownership, and use of data and applications. Copyrights and trade secrets are legal devices to protect the rights of developers and owners of information applications and data. Third, laws involve actions that can be taken by an organization to protect the secrecy, integrity, and availability of information and electronic services. Laws do not always provide an adequate control. They are slowly developing behind information technologies. They also do not face all irregular acts and cyber crimes committed on information and communication systems.

Progressively security services are becoming measurable like any tangible service, or a software package. Security services do have prices, but unlike tangible objects, they can be sold again and again and since the costs to reproduce them are very low, they often are transferred intangibly. However, security policy building, risk analysis, solution configuration, and personal training should be addressed appropriately with each enterprise. This shows that security services measurability is a hard task. In addition, security services can be hacked; meanwhile they should be able to be used for tracing and investigating evidences of attacks.

All these properties of information have an essential effect on the legal treatment of information. In that, there is a need for a legal basis for the protection of information.

Software privacy is the first example in which the value of information can be readily copied. Several approaches have been attempted to ensure that the software developer or publisher receives just compensation for use of his/her software. None of these approaches seem ideal. Therefore, it is likely that the availability of a complete legal frame will be needed, by any country, in addition to the technological issues.

Electronic publishing, protection of networked databases, and electronic commerce portals are important areas where legal issues must be solved as we move into an age of electronic business/economy. Ensuring for example that the electronic publisher receives fair compensation for his/her work, means that cryptographic-based technical solutions must be supported by a legal structure capable of defining the acceptable technical requirements to perform legal signature or encrypt documents.

The law managing electronic contracts and e-employment is hard to address, even though employees, objects, and contracts are practically standard entities for which legal precedents have been developed. The definitions of copyright and patent law are stressed when applied to computing and communication because old forms must be transformed to fit new objects. For these situations, however, cases and prototypes have been decided. Now they are establishing legal precedents and studies. Nevertheless, cyber crimes represent an area of the law that is less clear than other areas.

The legal system has explicit rules of what constitutes property. Generally, property is tangible, unlike sequences of bits. Getting a copy of (part of) a sensitive file or accessing unauthorized a computing system should be considered as a cyber crime. However, because "*access and copy*" operations are not physical objects, some courts in various countries are unenthusiastic to consider this as a theft. Adding to the problem of a rapidly changing technology, a computer can perform many roles in a cyber crime. A computer can be the subject or the medium of cyber crime since it can be attacked, used to attack, and used as a means to commit a cyber crime.

Cyber crimes statutes have to include a large spectrum of cases. But, even when it is acknowledged that a cyber crime has been committed, there are still several reasons why a cyber crime is hard to prosecute. This includes the need of understanding the cyber crime (computer literacy), finding evidences (e.g., tracing intrusions, and investigating disks), and evaluating assets and damages.

1.9 Summary

Security in business activity is an important issue that should be addressed appropriately by skilled people. This chapter provides guidance on the generic activities to be addressed when designing a security solution. In particular, this chapter helps organizations define, select, and document the nature and scope of the security services to be provided in order to protect business activity. Moreover, it discusses the basic functions needed to build up security services, how these functions work and interrelate, as well as the procedures necessary to implement these services.

This chapter is intended first to provide a self-contained resource to understand the role of policy security and risk management. Second, it provides managers responsible for the implementation, operation of service, and response to security incidents with a

high-level description of the main procedures to protect assets. Third, this chapter attempts to demonstrate the need for security services, skilled persons, and documented policies.

References

Allen, J. H. (2001). *CERT Guide to System and Network Security Practices*, The SEI Series in Software Engineering, Addison Wesley Professional.

Australian Computer Emergency Response Team. (2004). *2004 Australian Computer Crime and Security Survey* (available at www.auscert.org.au/download.html?f=114).

Gordon, L. A., M. P. Loed, W. Lucyshin, and R. Richardson. (2004) *2004 CSI/BFI Computer crime and security survey*, Computer Security Institute publications (available at www.gosci.com/forms/fbi/pdf.jhtml).

Hare, C. Policy development. In *Information Security Management Handbook*, volume 3, Tipton, H. F. and Krause M. (eds.). Auerbach, pp. 353–89.

Holbrook, P. and J. Reynolds. (1991). *Site Security Handbook* (available at www.securif.net/misc/Site_Security_Handbook).

Internet Engineering Task Force. (1997). *Site Security Handbook*, RFC 2196. IETF Network Working Group. Available at www.ietf.org/rfc/rfc2196.txt (date of access: Aug. 24th, 2004).

Obaidat, M. S. (1993b). A methodology for improving computer access security, *Computers Security Journal*, Vol. **12**, No. 7, 657–62.

Obaidat, M. S. and D. Macchairllo. (1993a). An on-line neural network system for computer access security. *IEEE Transactions on Industrial Electronics*, Vol. **40**, No. 2, 235–42.

Obaidat, M. S. and D. Macchairllo. (1994). A multilayer neural network system for computer access security, *IEEE Transactions on Systems, Man, and Cybernetics*, Vol. **24**, No. 5, 806–13.

Obaidat, M. S. and B. Sadoun. (1997). Verification of computer users using keystroke dynamics. *IEEE Transactions on Systems, Man and Cybernetics*, Part B, Vol. **27**, No. 2, 261–9.

Obaidat, M. S. and B. Sadoun. (1999). Keystroke dynamics based identification. In *Biometrics: Personal Identification in Networked Society*, Anil Jain *et al*. (eds.), Kluwer, pp. 213–29.

Stallings, W. (2001). *Cryptography and Network Security*, 3rd edn. Prentice Hall.

Swanson, M. (1998). *Developing Security Plans for Information Technology Systems*, NIST Special Publication 800–18.

West-Brown, M. J., D. Stikvoort, and K. P. Kossakowski. (1998). *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-98-HB-001). *Software Engineering Institute*, Carnegie Mellon University.