Computer Network Security Fundamentals 2

2.1 Introduction

Before we talk about network security, we need to understand in general terms what security is. Security is a continuous process of protecting an object from unauthorized access. It is as state of being or feeling protected from harm. That object in that state may be a person, an organization such as a business, or property such as a computer system or a file. Security comes from secure which means, according to *Webster Dictionary*, a state of being free from care, anxiety, or fear [1].

An object can be in a *physical state* of security or a *theoretical state* of security. In a physical state, a facility is secure if it is protected by a barrier like a fence, has secure areas both inside and outside, and can resist penetration by intruders. This state of security can be guaranteed if the following four protection mechanisms are in place: deterrence, prevention, detection, and response [1, 2].

- *Deterrence* is usually the first line of defense against intruders who may try to gain access. It works by creating an atmosphere intended to frighten intruders. Sometimes this may involve warnings of severe consequences if security is breached.
- *Prevention* is the process of trying to stop intruders from gaining access to the resources of the system. Barriers include firewalls, demilitarized zones (DMZs), and the use of access items like keys, access cards, biometrics, and others to allow only authorized users to use and access a facility.
- *Detection* occurs when the intruder has succeeded or is in the process of gaining access to the system. Signals from the detection process include alerts to the existence of an intruder. Sometimes, these alerts can be real time or stored for further analysis by the security personnel.
- *Response* is an aftereffect mechanism that tries to respond to the failure of the first three mechanisms. It works by trying to stop and/or prevent future damage or access to a facility.

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications
and Networks, DOI 10.1007/978-3-319-55606-2_2

The areas outside the protected system can be secured by wire and wall fencing, mounted noise or vibration sensors, security lighting, closed-circuit television (CCTV), buried seismic sensors, or different photoelectric and microwave systems [1]. Inside the system, security can be enhanced by using electronic barriers such as firewalls and passwords.

Digital barriers—commonly known as firewalls, discussed in detail in Chap. 12—can be used. Firewalls are hardware or software tools used to isolate the sensitive portions of an information system facility from the outside world and limit the potential damage by a malicious intruder.

A theoretical state of security, commonly known as pseudosecurity or security through obscurity (STO), is a false hope of security. Many believe that an object can be secured as long as nobody outside the core implementation group has knowledge about its existence. This security is often referred to as "bunk mentality" security. This is virtual security in the sense that it is not physically implemented like building walls, issuing passwords, or putting up a firewall, but it is effectively based solely on a philosophy. The philosophy itself relies on a need-to-know basis, implying that a person is not dangerous as long as that person doesn't have knowledge that could affect the security of the system like a network, for example. In real systems where this security philosophy is used, security is assured through a presumption that only those with responsibility and who are trustworthy can use the system and nobody else needs to know. So, in effect, the philosophy is based on the trust of those involved assuming that they will never leave. If they do, then that means the end of security for that system.

There are several examples where STO has been successfully used. These include Coca-Cola, KFC, and other companies that have, for generations, kept their secret recipes secure based on a few trusted employees. But the overall STO is a fallacy that has been used by many software producers when they hide their codes. Many times, STO hides system vulnerabilities and weaknesses. This was demonstrated vividly in Matt Blaze's 1994 discovery of a flaw in the Escrowed Encryption Standard (Clipper) that could be used to circumvent law-enforcement monitoring. Blaze's discovery allowed easier access to secure communication through the Clipper technology than was previously possible, without access to keys [3]. The belief that secrecy can make the system more secure is just a belief—a myth in fact. Unfortunately, the software industry still believes this myth.

Although its usefulness has declined as the computing environment has changed to large open systems, new networking programming, and network protocols, and as the computing power available to the average person has increased, the philosophy is in fact still favored by many agencies, including the military, many government agencies, and private businesses.

In either security state, many objects can be thought of as being secure if such a state, a condition, or a process is afforded to them. Because there are many of these objects, we are going to focus on the security of a few of these object models. These will be a computer, a computer network, and information.

2.1.1 Computer Security

This is a study, which is a branch of computer science, focusing on creating a secure environment for the use of computers. It is a focus on the "behavior of users," if you will, required and the protocols in order to create a secure environment for anyone using computers. This field, therefore, involves four areas of interest: the study of computer ethics, the development of both software and hardware protocols, and the development of best practices. It is a complex field of study involving detailed mathematical designs of cryptographic protocols. We are not focusing on this in this book.

2.1.2 Network Security

As we saw in Chap. 1, computer networks are distributed networks of computers that are either strongly connected meaning that they share a lot of resources from one central computer or loosely connected, meaning that they share only those resources that can make the network work. When we talk about computer network security, our focus object model has now changed. It is no longer one computer but a network. So computer network security is a broader study of computer security. It is still a branch of computer science, but a lot broader than that of computer security. It involves creating an environment in which a computer network, including all its resources, which are many; all the data in it both in storage and in transit; and all its users are secure. Because it is wider than computer security, this is a more complex field of study than computer security involving more detailed mathematical designs of cryptographic, communication, transport, and exchange protocols and best practices. This book focuses on this field of study.

2.1.3 Information Security

Information security is even a bigger field of study including computer and computer network security. This study is found in a variety of disciplines, including computer science, business management, information studies, and engineering. It involves the creation of a state in which information and data are secure. In this model, information or data is either in motion through the communication channels or in storage in databases on server. This, therefore, involves the study of not only more detailed mathematical designs of cryptographic, communication, transport, and exchange protocols and best practices but also the state of both data and information in motion. We are not discussing these in this book.

2.2 Securing the Computer Network

Creating security in the computer network model we are embarking on in this book means creating secure environments for a variety of resources. In this model, a resource is secure, based on the above definition, if that resource is protected from both internal and external unauthorized access. These resources, physical or not, are objects. Ensuring the security of an object means protecting the object from unauthorized access both from within the object and externally. In short, we protect objects. System objects are either tangible or nontangible. In a computer network model, the tangible objects are the hardware resources in the system, and the intangible object is the information and data in the system, both in transition and static in storage.

2.2.1 Hardware

Protecting hardware resources include protecting:

- End user objects that include the user interface hardware components such as all client system input components, including a keyboard, mouse, touchscreen, light pens, and others
- Network objects like firewalls, hubs, switches, routers, and gateways which are vulnerable to hackers
- Network communication channels to prevent eavesdroppers from intercepting network communications

2.2.2 Software

Protecting software resources includes protecting hardware-based software, operating systems, server protocols, browsers, application software, and intellectual property stored on network storage disks and databases. It also involves protecting client software such as investment portfolios, financial data, real estate records, images or pictures, and other personal files commonly stored on home and business computers.

2.3 Forms of Protection

Now, we know what model objects are or need to be protected. Let us briefly, keep details for later, survey ways and forms of protecting these objects. Prevention of unauthorized access to system resources is achieved through a number of services that include access control, authentication, confidentiality, integrity, and nonrepudiation.

2.3.1 Access Control

This is a service the system uses, together with a user pre-provided identification information such as a password, to determine who uses what of its services. Let us look at some forms of access control based on hardware and software.

2.3.1.1 Hardware Access Control Systems

Rapid advances in technology have resulted in efficient access control tools that are open and flexible, while at the same time ensuring reasonable precautions against risks. Access control tools falling in this category include the following:

- Access terminal: Terminal access points have become very sophisticated, and now they not only carry out user identification but also verify access rights, control access points, and communicate with host computers. These activities can be done in a variety of ways including fingerprint verification and real-time anti-break-in sensors. Network technology has made it possible for these units to be connected to a monitoring network or remain in a stand-alone off-line mode.
- Visual event monitoring: This is a combination of many technologies into one very useful and rapidly growing form of access control using a variety of real-time technologies including video and audio signals, aerial photographs, and Global Positioning System (GPS) technology to identify locations.
- Identification cards: Sometimes called proximity cards, these cards have become very common these days as a means of access control in buildings, financial institutions, and other restricted areas. The cards come in a variety of forms, including magnetic, bar coded, contact chip, and a combination of these.
- Biometric identification: This is perhaps the fastest growing form of control access tool today. Some of the most popular forms include fingerprint, iris, and voice recognition. However, fingerprint recognition offers a higher level of security.
- Video surveillance: This is a replacement of CCTV of yesteryear, and it is gaining popularity as an access control tool. With fast networking technologies and digital cameras, images can now be taken and analyzed very quickly and action taken in minutes.

2.3.1.2 Software Access Control Systems

Software access control falls into two types: point-of-access monitoring and remote monitoring. In *point of access* (POA), personal activities can be monitored by a PC-based application. The application can even be connected to a network or to a designated machine or machines. The application collects and stores access events and other events connected to the system operation and download access rights to access terminals.

In remote mode, the terminals can be linked in a variety of ways, including the use of modems, telephone lines, and all forms of wireless connections. Such terminals may, sometimes if needed, have an automatic calling at preset times if desired or have an attendant to report regularly.

2.3.2 Authentication

Authentication is a service used to identify a user. User identity, especially of remote users, is difficult because many users, especially those intending to cause harm, may masquerade as the legitimate users when they actually are not. This service provides a system with the capability to verify that a user is the very one he or she claims to be based on what the user is, knows, and has.

Physically, we can authenticate users or user surrogates based on checking one or more of the following user items [2]:

- Username (sometimes screen name).
- Password.
- *Retinal images*: The user looks into an electronic device that maps his or her eye retina image; the system then compares this map with a similar map stored on the system.
- *Fingerprints*: The user presses on or sometimes inserts a particular finger into a device that makes a copy of the user fingerprint and then compares it with a similar image on the system user file.
- *Physical location*: The physical location of the system initiating an entry request is checked to ensure that a request is actually originating from a known and authorized location. In networks, to check the authenticity of a client's location, a network or Internet Protocol (IP) address of the client machine is compared with the one on the system user file. This method is used mostly in addition to other security measures because it alone cannot guarantee security. If used alone, it provides access to the requested system to anybody who has access to the client machine.
- *Identity cards*: Increasingly, cards are being used as authenticating documents. Whoever is the carrier of the card gains access to the requested system. As is the case with physical location authentication, card authentication is usually used as a second-level authentication tool because whoever has access to the card automatically can gain access to the requested system.

2.3.3 Confidentiality

The confidentiality service protects system data and information from unauthorized disclosure. When data leave one extreme of a system such as a client's computer in a network, it ventures out into a nontrusting environment. So, the recipient of that data may not fully trust that no third party like a cryptanalysis or a man in the middle has eavesdropped on the data. This service uses encryption algorithms to ensure that nothing of the sort happened while the data was in the wild.

Encryption protects the communications channel from sniffers. *Sniffers* are programs written for and installed on the communication channels to eavesdrop on network traffic, examining all traffic on selected network segments. Sniffers are easy to write and install and difficult to detect. The encryption process uses an encryption algorithm and key to transform data at the source, called *plaintext*; turn it into an encrypted form called *ciphertext*, usually unintelligible form; and finally recover it at the sink. The encryption algorithm can either be *symmetric* or *asymmetric*. Symmetric encryption or secret key encryption, as it is usually called, uses a common key and the same cryptographic algorithm to scramble and unscramble the message. Asymmetric encryption commonly known as public key encryption uses two different keys: a public key known by all and a private key known by only the sender and the receiver. Both the sender and the receiver have a pair of these keys, one public and one private. To encrypt a message, a sender uses the receiver's public key which was published. Upon receipt, the recipient of the message decrypts it with his or her private key.

2.3.4 Integrity

The integrity service protects data against active threats such as those that may alter it. Just like data confidentiality, data in transition between the sending and receiving parties is susceptible to many threats from hackers, eavesdroppers, and cryptanalysts whose goal is to intercept the data and alter it based on their motives. This service, through encryption and *hashing algorithms*, ensures that the integrity of the transient data is intact. A hash function takes an input message M and creates a code from it. The code is commonly referred to as a hash or a message digest. A one-way hash function is used to create a signature of the message—just like a human fingerprint. The hash function is, therefore, used to provide the message's integrity and authenticity. The signature is then attached to the message before it is sent by the sender to the recipient.

2.3.5 Nonrepudiation

This is a security service that provides proof of origin and delivery of service and/or information. In real life, it is possible that the sender may deny the ownership of the exchanged digital data that originated from him or her. This service, through *digital signature* and encryption algorithms, ensures that digital data may not be repudiated by providing proof of origin that is difficult to deny. A digital signature is a cryptographic mechanism that is the electronic equivalent of a written signature to authenticate a piece of data as to the identity of the sender.

We have to be careful here because the term "nonrepudiation" has two meanings, one in the legal world and the other in the cryptotechnical world. Adrian McCullagh and Willian Caelli define "nonrepudiation" in a cryptotechnical way as follows [4]:

- In authentication, a service that provides proof of the integrity and origin of data, both in a forgery-proof relationship, which can be verified by any third party at any time

- In authentication, an authentication that with high assurance can be asserted to be genuine and that cannot subsequently be refuted

However, in the legal world, there is always a basis for repudiation. This basis, again according to Adrian McCullagh, can be as follows:

- The signature is a forgery.
- The signature is not a forgery, but was obtained via:
  - Unconscionable conduct by a party to a transaction
  - Fraud instigated by a third party
  - Undue influence exerted by a third party

We will use the cryptotechnical definition throughout the book. To achieve nonrepudiation, users and application environments require a *nonrepudiation service* to collect, maintain, and make available the irrefutable evidence. The best services for nonrepudiation are digital signatures and encryption. These services offer trust by generating unforgettable evidence of transactions that can be used for dispute resolution after the fact.

2.4 Security Standards

The computer network model also suffers from the standardization problem. Security protocols, solutions, and best practices that can secure the computer network model come in many different types and use different technologies resulting in incompatibility of interfaces (more in Chap. 16), less interoperability, and uniformity among the many system resources with differing technologies within the system and between systems. System managers, security chiefs, and experts, therefore, choose or prefer standards, if no de facto standard exists, that are based on service, industry, size, or mission. The type of service offered by an organization determines the types of security standards used. Like service, the nature of the industry an organization is in also determines the types of services offered by the system, which in turn determines the type of standards to adopt. The size of an organization also determines what type of standards to adopt. In relatively small establishments, the ease of implementation and running of the system influence the standards to be adopted. Finally, the mission of the establishment also determines the types of standards used. For example, government agencies have a mission that differs from that of a university. These two organizations, therefore, may choose different standards. We are, therefore, going to discuss security standards along these divisions. Before we do that, however, let us look at the bodies and organizations behind the formulation, development, and maintenance of these standards. These bodies fall into the following categories:

- International organizations such as the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers (IEEE), the International

Organization for Standardization (ISO), and the International Telecommunications Union (ITU)

- Multinational organizations like the European Committee for Standardization (CEN), Commission of European Union (CEU), and European Telecommunications Standards Institute (ETSI)
- National governmental organizations like the National Institute of Standards and Technology (NIST), American National Standards Institute (ANSI), and Canadian Standards Council (CSC)
- Sector-specific organizations such as the European Committee for Banking Standards (ECBS), European Computer Manufacturers Association (ECMA), and Institute of Electrical and Electronics Engineers (IEEE)
- Industry standards such as RSA, the Open Group (OSF + X/Open), Object Management Group (OMG), World Wide Web Consortium (W3C), and the Organization for the Advancement of Structured Information Standards (OASIS)
- Other sources of standards in security and cryptography

Each one of these organizations has a set of standards. Table 2.1 shows some of these standards. In the table, x is any digit between 0 and 9.

2.4.1 Security Standards Based on Type of Service/Industry

System and security managers and users may choose a security standard to use based on the type of industry they are in and what type of services that industry provides. Table 2.2 shows some of these services and the corresponding security standards that can be used for these services.

Let us now give some details of some of these standards.

2.4.1.1 Public Key Cryptography Standards (PKCS)

In order to provide a basis and a catalyst for interoperable security based on public key cryptographic techniques, the Public Key Cryptography Standards (PKCS) were established. These are recent security standards, first published in 1991 following discussions of a small group of early adopters of public key technology. Since their establishment, they have become the basis for many formal standards and are implemented widely.

In general, PKCS are security specifications produced by RSA Laboratories in cooperation with secure system developers worldwide for the purpose of accelerating the deployment of public key cryptography. In fact, worldwide contributions from the PKCS series have become part of many formal and de facto standards, including ANSI X9 documents, PKIX, SET, S/MIME, and SSL.

2.4.1.2 The Standards for Interoperable Secure MIME (S/MIME)

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a specification for secure electronic messaging. It came to address a growing problem of e-mail

Table 2.1 Organizations and their standards

Organization	Standards
IETF	IPSec, XML-Signature XPath Filter 2, X.509, Kerberos, S/MIME, RFC 1108 US Department of Defense Security Options for the Internet Protocol, RFC 2196 Site Security Handbook, RFC 2222 Simple Authentication and Security Layer, RFC 2323 IETF Identification and Security Guidelines, RFC 2401 Security Architecture for the Internet Protocol, RFC 2411 IP Security Document Roadmap, RFC 2504 Users' Security Handbook, RFC 2828 Internet Security Glossary, RFC 3365 Strong Security Requirements for Internet Engineering Task Force Standard Protocols, RFC 3414 User-Based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), RFC 3631 Security Mechanisms for the Internet, RFC 3871 Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure, RFC 4033 DNS Security Introduction and Requirements, RFC 4251 The Secure Shell (SSH) Protocol Architecture, RFC 4301 Security Architecture for the Internet Protocol
ISO	ISO 7498-2:1989 Information processing systems—Open Systems Interconnection, ISO/IEC 979x, ISO/IEC 997, ISO/IEC 1011x, ISO/IEC 11xx, ISO/IEC DTR 13xxx, ISO/IEC DTR 14xxx
ITU	X.2xx, X.5xx, X.7xx, X.80x
ECBS	TR-40x
ECMA	ECMA-13x, ECMA-20x
NIST	X3 Information Processing, X9.xx Financial, X12.xx Electronic Data Exchange
IEEE	P1363 Standard Specifications for Public Key Cryptography, IEEE 802.xx, IEEE P802.11 g, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications
RSA	PKCS #x—Public key cryptographic standard
W3C	XML Encryption, XML Signature, exXensible Key Management Specification (XKMS)

interception and forgery at the time of increasing digital communication. So, in 1995, several software vendors got together and created the S/MIME specification with the goal of making it easy to secure messages from prying eyes.

It works by building a security layer on top of the industry standard MIME protocol based on PKCS. The use of PKCS avails the user of S/MIME with immediate privacy, data integrity, and authentication of an e-mail package. This has given the standard a wide appeal, leading to S/MIME moving beyond just e-mail. Already vendor software warehouses, including Microsoft, Lotus, and Banyan, and other online electronic commerce services are using S/MIME.

2.4.1.3 Federal Information Processing Standards (FIPS)

Federal Information Processing Standards (FIPS) are National Institute of Standards and Technology (NIST)-approved standards for advanced encryption. These are US federal government standards and guidelines in a variety of areas in data processing. They are recommended by NIST to be used by the US government organizations and others in the private sector to protect sensitive information. They range from FIPS 31 issued in 1974 to current FIPS 198.

Table 2.2 Security standards based on services

Area of application	Service	Security standard
Internet security	Network authentication	Kerberos
	Secure TCP/IP communications over the Internet	IPsec
	Privacy-enhanced electronic mail	S/MIME, PGP
	Public Key Cryptography Standards	3DES, DSA, RSA, MD5, SHA-1, PKCS
	Secure Hypertext Transfer Protocol	S-HTTP
	Authentication of directory users	X.509/ISO/IEC 9594-8:2000
	Security protocol for privacy on Internet/transport security	SSL, TLS, SET
Digital signature and encryption	Advanced encryption standard/ PKI/ digital certificates, XML digital signatures	X.509, RSA BSAFE SecurXML-C, DES, AES, DSS/DSA, EESSI, ISO 9xxx, ISO, SHA/SHS, XML digital signatures (XML-DSIG), XML Encryption (XMLENC), XML Key Management Specification (XKMS)
Login and authentication	Authentication of user's right to use system or network resources.	SAML, Liberty Alliance, FIPS 112
Firewall and system security	Security of local, wide, and metropolitan area networks	Secure Data Exchange (SDE) protocol for IEEE 802, ISO/IEC 10164

2.4.1.4 Secure Sockets Layer (SSL)

SSL is an encryption standard for most Web transactions. In fact, it is becoming the most popular type of e-commerce encryption. Most conventional intranet and extranet applications would typically require a combination of security mechanisms that include

- Encryption
- Authentication
- Access control

SSL provides the encryption component implemented within the TCP/IP. Developed by Netscape Communications, SSL provides secure Web client and server communications, including encryption, authentication, and integrity checking for a TCP/IP connection.

2.4.1.5 Web Services Security Standards

In order for Web transactions such as e-commerce to really take off, customers will need to see an open architectural model backed up by a standards-based security framework. Security players, including standards organizations, must provide that open model and a framework that is interoperable, that is, as vendor neutral as possible, and able to resolve critical, often sensitive, issues related to security. The security framework must also include Web interoperability standards for access control, provisioning, biometrics, and digital rights.

To meet the challenges of Web security, two industry rival standards companies are developing new standards for XML digital signatures that include XML Encryption, XML Signature, and exXensible Key Management Specification (XKMS) by the World Wide Web Consortium (W3C), and BSAFE SecurXML-C software development kit (SDK) for implementing XML digital signatures by rival RSA Security. In addition, RSA also offers a Security Assertion Markup Language (SAML) specification, an XML framework for exchanging authentication, and authorization information. It is designed to enable secure single sign-on across portals within and across organizations.

2.4.2 Security Standards Based on Size/Implementation

If the network is small or it is a small organization such as a university, for example, security standards can be spelled out as either the organization's security policy or its best practices on the security of the system, including the physical security of equipment, system software, and application software:

- Physical security: This emphasizes the need for security of computers running the Web servers and how these machines should be kept physically secured in a locked area. Standards are also needed for backup storage media like tapes and removable disks.
- Operating systems: The emphasis here is on privileges and number of accounts, and security standards are set based on these. For example, the number of users with most privileged access like *root* in Unix or *Administrator* in NT should be kept to a minimum. Set standards for privileged users. Keep to a minimum the number of user accounts on the system. State the number of services offered to clients computers by the server, keeping them to a minimum. Set a standard for authentication such as user passwords and for applying security patches.
- System logs: Logs always contain sensitive information such as dates and times of user access. Logs containing sensitive information should be accessible only to authorized staff and should not be publicly accessible. Set a standard on who and when logs should be viewed and analyzed.
- Data security: Set a standard for dealing with files that contain sensitive data. For example, files containing sensitive data should be encrypted wherever possible using strong encryption or should be transferred as soon as possible and practical to a secured system not providing public services.

As an example, Table 2.3 shows how such standards may be set.

Table 2.3 Best security practices for a small organization

Application area	Security standards
Operating systems	Unix, Linux, Windows, etc.
Virus protection	Norton
E-mail	PGP, S/MIME
Firewalls	
Telnet and FTP terminal applications	SSH (secure shell)

2.4.3 Security Standards Based on Interests

In many cases, institutions and government agencies choose to pick a security standard based solely on the interest of the institution or the country. Table 2.4 below shows some security standards based on interest, and the subsections following the table also show security best practices and security standards based more on national interests.

2.4.3.1 British Standard 799 (BS 7799)

The BS 7799 standard outlines a code of practice for information security management that further helps to determine how to secure network systems. It puts forward a common framework that enables companies to develop, implement, and measure effective security management practice and provide confidence in intercompany trading. BS 7799 was first written in 1993, but it was not officially published until 1995, and it was published as an international standard BS ISO/IEC 17799:2000 in December 2000.

2.4.3.2 Orange Book

This is the US Department of Defense *Trusted Computer System Evaluation Criteria* (DOD-5200.28-STD) standard known as the *Orange Book*. For a long time, it has been the de facto standard for computer security used in government and industry, but as we will see in Chap. 15, other standards have now been developed to either supplement it or replace it. First published in 1983, its security levels are referred to as "Rainbow Series."

2.4.4 Security Best Practices

As you noticed from our discussion, there is a rich repertoire of standards security tools on the system and information security landscape because as technology evolves, the security situation becomes more complex and it grows more so every day. With these changes, however, some trends and approaches to security remain the same. One of these constants is having a sound strategy of dealing with the changing security landscape. Developing such a security strategy involves keeping an eye on the reality of the changing technology scene and rapidly increasing security threats. To keep abreast of all these changes, security experts and security

Table 2.4 Interest-based security standards

Area of application	Service	Security standard
Banking	Security within banking IT systems	ISO 8730, ISO 8732, ISO/TR 17944
Financial	Security of financial services	ANSI X9.x, ANSI X9.xx

managers must know how and what to protect and what controls to put in place and at what time. It takes security management, planning, policy development, and the design of security procedures. It's important to remember and definitely understand that there is no procedure, policy, or technology, however much you like it and trust it, that will ever be 100%, so it is important for a company preferably to have a designated security person, a security program officer, and chief security officer (CSO), under the chief information officer (CIO), and to be responsible for the security best practices. Here are some examples of best practices.

Commonly Accepted Security Practices and Regulations (CASPR) Developed by the CASPR Project, this effort aims to provide a set of best practices that can be universally applied to any organization regardless of industry, size or mission. Such best practices would, for example, come from the world's experts in information security. CASPR distills the knowledge into a series of papers and publishes them so they are freely available on the Internet to everyone. The project covers a wide area, including operating system and system security, network and telecommunication security, access control and authentication, infosecurity management, infosecurity auditing and assessment, infosecurity logging and monitoring, application security, application and system development, and investigations and forensics. In order to distribute their papers freely, the founders of CASPR use the open source movement as a guide, and they release the papers under the GNU Free Document License to make sure they and any derivatives remain freely available.

Control Objectives for Information and (Related) Technology (COBIT) Developed by IT auditors and made available through the Information Systems Audit and Control Association, COBIT provides a framework for assessing a security program. COBIT is an open standard for control of information technology. The IT Governance Institute has, together with the worldwide industry experts, analysts, and academics, developed new definitions for COBIT that consist of maturity models, critical success factors (CSFs), key goal indicators (KGIs), and key performance indicators (KPIs). COBIT was designed to help three distinct audiences [5]:

- Management who needs to balance risk and control investment in an often unpredictable IT environment

- Users who need to obtain assurance on the security and controls of the IT services upon which they depend to deliver their products and services to internal and external customers
- Auditors who can use it to substantiate their opinions and/or provide advice to management on internal controls

Operationally Critical Threat, Asset, and Vulnerability Evaluation (*OCTAVE*) by Carnegie Mellon's CERT Coordination Center: OCTAVE is an approach for self- directed information security risk evaluations that [6]:

- Puts organizations in charge
- Balances critical information assets, business needs, threats, and vulnerabilities
- Measures the organization against known or accepted good security practices
- Establishes an organization-wide protection strategy and information security risk mitigation plans

In short, it provides measures based on accepted best practices for evaluating security programs. It does this in three phases:

- It determines information assets that must be protected.
- It evaluates the technology infrastructure to determine if it can protect those assets and how vulnerable it is and defines the risks to critical assets.
- It uses good security practices and establishes an organization-wide protection strategy and mitigation plans for specific risks to critical assets.

General Best Practices—Matthew Putvinski, in his article *IT Security Series Part 1: Information Security Best Practices* [7], discusses under the following general categories:

- Chief information security officer or designate: Establish the need for a security designated officer to oversee security-related issues in the enterprise because the lack of a person responsible for security in any organization means the organization does not give information security priority.
- End user: The security guidelines here must be contained in the organization's security policy of what the organization's end users must and must not do as far as dealing with organization's information in general and computing services in particular. As we move into miniature mobile devices and if a policy is to use a bring-your-own-device (BYOD), specific data handling policies must be in place.
- Software updates and patches: Specific guidelines in the organization security policy book must specifically take a stance on how the organization will use software security patches and upgrades and the frequency of updates.
- Vendor management: If the organization is using software provided by third-party individuals or organizations as vendors, care must be taken to ensure that

any organization's confidential information provided to vendors to help identify a suitable software tool is well documented and indicated to whom.

- Physical security: This is squarely a security policy issue specifically spelling out the physical specification required to safeguard the organization's information and data. These include access to offices and digital equipment, when and where information is stored, and when and where information is destroyed. We will discuss more of this in the coming chapters.
- The following guidelines are also a security policy issues:
  - Data classification and retention
  - Password requirements and guidelines
  - Wireless networking
  - Mobile device usage and access
  - Employee awareness training
  - Incident response

Exercises

1. What is security and information security? What is the difference?
2. It has been stated that security is a continuous process; what are the states in this process?
3. What are the differences between symmetric and asymmetric key systems?
4. What is PKI? Why is it so important in information security?
5. What is the difference between authentication and nonrepudiation?
6. Why is there a dispute between digital nonrepudiation and legal nonrepudiation?
7. Virtual security seems to work in some systems. Why is this so? Can you apply it in a network environment? Support your response.
8. Security best practices are security guidelines and policies aimed at enhancing system security. Can they work without known and proven security mechanisms?
9. Does information confidentiality infer information integrity? Explain your response.
10. What are the best security mechanisms to ensure information confidentiality?

Advanced Exercises

1. In the chapter, we have classified security standards based on industry, size, and mission. What other classifications can you make and why?
2. Most of the encryption standards that are being used such as RSA and DES have not been formally proven to be safe. Why then do we take them to be secure—what evidence do we have?
3. IPsec provides security at the network layer. What other security mechanism is applicable at the network layer? Do network layer security solutions offer better security?

4. Discuss two security mechanisms applied at the application layer. Are they safer than those applied at the lower network layer? Support your response.
5. Are there security mechanisms applicable at transport layer? Is it safer?
6. Discuss the difficulties encountered in enforcing security best practices.
7. Some security experts do not believe in security policies. Do you? Why or why not?
8. Security standards are changing daily. Is it wise to pick a security standard then? Why or why not?
9. If you are an enterprise security chief, how would you go about choosing a security best practice? Is it good security policy to always use a best security practice? What are the benefits of using a best practice?
10. Why it is important to have a security plan despite the various views of security experts concerning its importance?

References

1. Kizza JM (2003) Social and ethical issues in the information age, 2nd edn. Springer, New York
2. Scherphier A. CS596 Client-server programming security. http://www.sdsu.edu/cs596/security.html
3. Mercuri R, Neumann P Security by obscurity. Commun ACM 46(11):160
4. McCullagh A, Caelli W Non-repudiation in the digital environment. http://www.firstmonday.dk/issues/issue5_8/mccullagh/index.html#author
5. CobiT a Practical Toolkit for IT Governance. http://www.ncc.co.uk/ncc/myitadviser/archive/issue8/business_processes.cfm
6. OCTAVE: Information Security Risk Evaluation. http://www.cert.org/octave/
7. Putvinski M. IT security series part 1: information security best practices. http://www.corporatecomplianceinsights.com/information-security-best-practices