

Chapter 1

Survey of Secure Computing

Kuruvilla Mathew and Biju Issac

Contents

1.1	Related Works.....	2
1.2	Introduction.....	3
1.3	About Information Systems and Security and Applicable Areas	4
1.3.1	The Basics	4
1.3.2	Cryptography to the Rescue.....	4
1.4	Challenges in Information Security versus Traditional Security	5
1.5	Areas in Secure Computing.....	5
1.5.1	Protocol Attacks and Prevention, Secure Protocols	6
1.5.1.1	TCP Sequence Number Prediction Attack	6
1.5.1.2	Routing Protocol Attacks.....	7
1.5.1.3	Server Attacks.....	8
1.5.1.4	Some Other Services/Protocols	9
1.5.1.5	Trivial Issues.....	10
1.5.2	DoS and Distributed DoS	11
1.5.2.1	Background	11
1.5.2.2	DoS and Distributed DoS Attacks.....	11
1.5.2.3	DoS and DDoS Attack Defenses	12
1.5.3	Botnets	13
1.5.4	Database, Web, and Cloud Security	13
1.5.4.1	Database Security	14
1.5.4.2	Web Security	15
1.5.4.3	Cloud Computing and Security.....	17
1.5.5	Mobile and Wireless (Including Android and Smart Devices)	18
1.5.5.1	About Mobile Security: Definition and Need	18
1.5.5.2	Categories of Attacks on Mobile Devices.....	19
1.5.6	Social Media and Social Aspects of Computer Security	21
1.5.7	Multimedia Security	21

1.5.7.1	Special Features of Multimedia.....	22
1.5.7.2	Encryption in Multimedia.....	22
1.6	Defenses in Secure Computing	22
1.6.1	Security Policy, Model Architectures, and so Forth	22
1.6.1.1	Defense In-Depth Model.....	22
1.6.1.2	Access Control Models	23
1.6.2	Cryptography and Steganography.....	23
1.6.3	Firewalls	23
1.6.4	Intrusion Detection Systems.....	24
1.6.5	People, Policies, Procedures, and Practices.....	24
1.7	Summary and Conclusion.....	24
	References	24

Personal computers brought about a revolution in the use of general-purpose computers. They moved into homes and offices, and more and more people began using them, putting more and more data onto computing systems. The fact that protocols and systems were never designed to cater to this explosion in adapting the computing systems also left much vulnerability in the systems, which created threats in the computing realm. Then started parallel efforts to secure existing infrastructure, with the aim to provide three main components of security in computing, namely, confidentiality, integrity, and availability. The difference in the threats and exploits of the digital world makes traditional systems of secure measures fall short, and it is required to provide digital defense mechanisms to ensure secure computing. Secure computing spans a wide spectrum of areas, including protocol-based security issues, denial of service, web and cloud, mobile, database, and social- and multimedia-related security issues, just to name a few. Even as threats present themselves, active mechanisms and good preparation can help to minimize incidents and losses arising from them, but it is also to be noted that security in computing is still a long way from complete. This chapter aims at presenting a survey of common issues in security attacks and defenses in computing through the application of cryptography and the aid of security models for securing systems.

1.1 Related Works

Peng et al. (2007) present a survey of network-based defense mechanisms countering the denial-of-service (DoS) and distributed DoS (DDoS) problems. This paper looks at the DoS and DDoS attacks and the possible defenses in research and practice. Furht and Kirovski (2005) have authored the *Multimedia Security Handbook*, which presents security issues in relation with multimedia. Multimedia is different from normal digital content and requires a different approach to security. Smith et al. (2004) present “Cyber Criminals on Trial,” in which they discuss the legal side of cybercrime and how geographical boundaries present a challenge in dealing with cybercrimes. Caldwell (2013) presents “Plugging the Cyber-Security Skills Gap,” in which he discusses how governmental policies and their intricacies can become a challenge in the advancement of cyber defense.

Harris and Hunt (1999) present a detailed discussion on Transmission Control Protocol/Internet Protocol (TCP/IP) security threats and attack methods. They discuss in detail TCP/IP issues, threats, and defenses. Bellare (1989) presents “Security Problems in the TCP/IP Protocol

Suite,” which details TCP/IP-related security problems. Morris (1985) presents “A Weakness in the 4.2 BSD Unix TCP/IP Software,” in particular, the TCP/IP security holes that make it vulnerable to attack, especially predicting TCP/IP sequence numbers. CERT (2006) presents statistics on security incidents reported and compiled. Chen et al. (2010) present “What’s New About Cloud Computing Security,” discussing some security threats posed by the newer developments in computing technology, like the cloud. Gil and Poletto (2001) present “MULTOPS: A Data-Structure for Bandwidth Attack Detection.” This discusses MULTOPS as a high-security system with mechanisms for defense built in.

Jajodia (1996) presents “Database Security and Privacy,” in which detailed database security and privacy issues are discussed. Data now mean more than text, which calls for more measures for their defense. Bertino and Sandhu (2005) present “Database Security—Concepts, Approaches, and Challenges,” in which more database-related issues are discussed. The use of access validation is also discussed in detail. Gollmann (2010) presents “Computer Security,” discussing detailed access control methods like mandatory access control and discretionary access control mechanisms. Bertino et al. (1995) present “Database Security: Research and Practice,” which provides more details on database security and related access control mechanisms (Bertino et al. 1995). Bertino (1998) presents “Data Security,” which also discusses databases and different methods of securing data.

Rubin and De Geer (1998) present a survey of web security. This paper looks at web security and its issues and various possible solutions in this paradigm. Subashini and Kavitha (2011) present a survey on security issues in service delivery models of cloud computing. This paper surveys various issues pertaining to the cloud-based service model and some mechanisms for defense best practices. Becher et al. (2011) present “Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices,” in which various security-related issues pertaining to mobile devices in particular are discussed. The paper discusses how mobile issues are not as prevalent as expected, possibly due to better best practices in securing the underlying protocols and systems.

Khatrri et al. (2009) present a survey on security issues in mobile ad hoc networks, discussing works on ad hoc mobile networks and their security issues. Irani et al. (2011) present “Reverse Social Engineering Attacks in Online Social Networks,” in which they discuss reverse social engineering attacks using forged identities and other methods over online social networks. Workman (2007) presents “Gaining Access with Social Engineering,” which discusses how social engineering attacks make unsuspecting victims prey to their schemes through social engineering attack to gain access to systems. The Microsoft Security Content Overview can present some good security models as defense against several threats using good practices and models. Tang et al. (2012) discuss detection and prevention of Session Initiation Protocol (SIP) flooding attacks in voice over IP (VoIP) networks. The SIP flooding attack floods the network with SIP packets, negatively affecting the VoIP service and generating a kind of DoS attack.

1.2 Introduction

A computer as a personal device was not even a dream in the pre-1980s, but after less than 30 years, we now see them in the hands of children. The original intended use of computers was within confined spaces, by expert users. The advent of personal computers with public widespread access to the Internet has radically changed this, bringing knowledge, information, and connectivity to everyone with access. This has brought, along with the convenience, risks as well, as

resources are equally accessible for people with malicious intent. The Morris Worm in 1988 was the first major security incident on the Internet (Peng et al. 2007).

The issue has awakened the call for security in computing, which is a very wide domain. This chapter on computer security identifies some of the fundamental reasons, issues, and approaches towards making computers and networks a “safe” place for everyone.

1.3 About Information Systems and Security and Applicable Areas

1.3.1 The Basics

The computer is now in use in all domains, including military, medicine, research, governments, banks, businesses and services, art, and social interactions. This puts a vast amount of sensitive and confidential data on computers and computer networks, which can be largely destructive if they fall into the wrong hands. This makes computer security a topic of prime importance. However, computer security is not the same as securing gold. One cannot achieve computer security by locking up a server or a PC in a safety vault placed under armed security guards. Security in computing involves ensuring that the data and systems are accessible to those and only to those who are authorized to access them and ensuring that they are preserved without changes while in storage and transit over the network. Hence, computer security must essentially ensure three elements—(1) confidentiality, (2) integrity, and (3) availability. Confidentiality implies that the data and the systems are maintained a secret from all who are not authorized to access them; integrity maintains that they are preserved as expected and not modified (intentionally or otherwise) while in storage, transit over the network, and so forth; and availability ensures that the data, services, or systems are available to legitimate users. It is the goal of any security system in computing to ensure that all three are at acceptable levels.

1.3.2 Cryptography to the Rescue

Confidentiality, keeping data secret, is often attained by using cryptography, which will ensure that data are sufficiently obscured in storage and in transit and can be read only by authorized users. The data to be encrypted are transformed using some encryption algorithm based on some secret value, which legitimate users use to gain access, applying a reverse process of the algorithm to retrieve the original data. The processes are called encryption and decryption, respectively, and they work as follows.

The message for encryption is called *plaintext*, which passes through an *encryption function* on a key Ke , and the resultant message is called *ciphertext*, which can be transmitted or stored in a nonsecure channel or medium. A good ciphertext is one from which it is reasonably difficult to guess the plaintext. To recover the plaintext, the ciphertext is passed through the *decryption function* with the key Kd . For symmetric key encryption, the same key is used to encrypt and decrypt a message ($Ke = Kd$), and asymmetric key encryption or a public-key cipher uses different keys ($Ke \neq Kd$) for each (Furht and Kirovski 2005) (Figure 1.1).

There are two key types of ciphers, block ciphers and stream ciphers. The block cipher divides the message into equal-size blocks and encrypts each of them, but this may leave patterns. Stream ciphers work on the source, dividing the message with random sequences derived from the

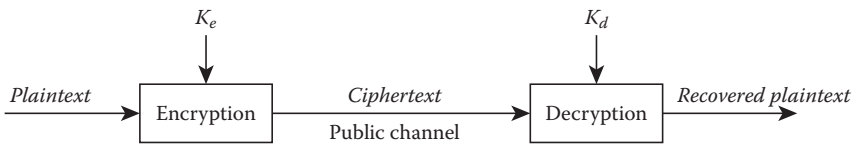


Figure 1.1 Encryption and decryption of a cipher.

key, hence making it completely obscure. In cryptography, the strength of the cipher is usually dependent on the strength of the key.

1.4 Challenges in Information Security versus Traditional Security

Information security–related crime is quite different from crime in the traditional aspect owing mainly to the nature of the crime. A theft in a traditional security system is visible as the stolen item changes hands, whereas information systems can be copied on electronic media, leaving the original working system intact and the theft unnoticed. The absence of clarity in legal provisions makes admission of digital evidence either difficult or impossible. The differences in cross-jurisdiction approaches make it almost impossible to deal with issues of international origin, which is more pronounced in information security as cyber users transcend geographical boundaries (Smith et al. 2004). The Computer Misuse Act of 1990, amended by the Police and Justice Act of 2006, makes developing, possessing, and/or obtaining articles for use in computer misuse offense a crime, which also includes tools of legitimate security professionals, such as network mappers, which further restrict the advancement of cyber security (Caldwell 2013).

Detailed discussion on this is legal in nature and falls under the banner of cyber laws and, hence, outside the scope of this chapter. However, it is worth mentioning that computer security incidents have constantly been on the rise in the absence of legal systems for identifying, implicating, and taking punitive action against perpetrators of such incidents.

1.5 Areas in Secure Computing

Secure computing is a wide-open domain reaching many dimensions. The nature of attacks can vary from amateur attempts out of curiosity or for popularity to pranks and tricks to more serious criminal activities involving serious financial implications and fraud. In order to address the expansive breadth of challenges, we will organize the remainder of this discussion as follows.

- Protocol attacks: Exploiting inherent weaknesses in protocols.
- Denial-of-service (DoS) attacks: Attempts to overwhelm public access systems or services to the point of resource exhaustion to deny legitimate access.
- Botnets: Networks of compromised/unsuspecting hosts on which an attacker gains and maintains control. They can then make use of these to launch many kinds of attacks (mainly DoS).

- Database web and cloud security: Regarding securing databases, web applications, and cloud access.
- Mobile and wireless security: Issues and attacks in mobile computing, including those in the Wi-Fi and smartphone arena.
- Social media and social aspects of computer security: The social networking media and related issues as well as social engineering attacks.
- Multimedia security: Security in IP-based media services including images, audio, paid TV channels, movies, voice over IP (VoIP), and many more.

1.5.1 Protocol Attacks and Prevention, Secure Protocols

The TCP/IP protocol suite, developed under the sponsorship of the Department of Defense, had a number of inherent flaws. In this section, we will explore some of the most popular vulnerabilities that were exploited by the attackers to cause security breaches.

1.5.1.1 TCP Sequence Number Prediction Attack

1.5.1.1.1 The Attack

The normal TCP connection works by the establishment of a three-way handshake (Harris and Hunt 1999), shown as follows. A client initiates a request with a more-or-less random initial sequence number (ISN_c). A server acknowledges the ISN_c and, with its initial sequence number (ISN_s), creates a half-open connection (Bellovin 1989; Harris and Hunt 1999). The client acknowledges (ACK) this, establishing a trusted connection, after which they start data exchange (Bellovin 1989).

```

C → S : SIN(ISNc)
S → C : SYN(ISNs), ACK(ISNc)
C → S : ACK(ISNs)
C → S : data
and/or
S → C : data

```

If an attacker (X) has an opportunity to predict the ISN, then the attacker tries to impersonate T. Even though the reply does not return to X, it still can send in data to the server and take over an established trusted connection (Bellovin 1989).

```

A → S : SYN(ISNx), SRC = T
S → T : SYN(ISNs), ACK(ISNx)
A → S : ACK(ISNs), SRC = T
A → S : A CK(ISNs), SRC = T, nasty-data

```

The target T, also called “forged” or “spoofed” host, can be overwhelmed with connection requests so that it does not send the reset (RST) signal to terminate invalid connections. If the attack host (X) can predict the ISN, then it can send synchronization (SYN) packets to B. Even

though its response does not reach A, A is able to send data to the server. If the protocol allows command execution, then the attacker has access to the server (Bellovin 1989). The fact that it is actually possible to predict the ISN with a high degree of confidence in Berkeley systems was pointed out by Morris (1985).

1.5.1.1.2 The Defense

This issue becomes less prominent as the ISN becomes increasingly complex to predict. Therefore, the defense against this is to make the ISN as random as possible. Another solution for this is to randomize the increment, making it difficult for attackers to carry on the communication. A simpler defense is to use cryptography for ISNs, with secret keys that cannot be broken in reasonably acceptable time frames (Bellovin 1989).

1.5.1.2 Routing Protocol Attacks

Many of the protocols were designed for providing seamless connectivity without much control on security, leaving much vulnerability. This section tries to look at the various attacks based on the specific routing protocols and their weaknesses.

1.5.1.2.1 Source Routing Attacks

1.5.1.2.1.1 The Attack — If the originator of the request is allowed to make use of source routing, then it allows the attacker to route return traffic to itself by specifying itself as the source router or return route. This is therefore a relatively simple method of attack (Bellovin 1989).

1.5.1.2.1.2 The Defense — This attack is rather difficult to defend other than by avoiding source routing completely or maintaining a trust list of gateways and accepting packets from these gateways only. If necessary, a firewall can filter external traffic from that with internal (trusted) network addresses. This, however, cannot work if the organization has multiple trusted networks with varying degrees of trust (Bellovin 1989).

1.5.1.2.2 Routing Information Protocol Attacks

1.5.1.2.2.1 The Attack — Routing Information Protocol (RIP) is used to dynamically advertise routes and is devoid of any authentication mechanisms. Attacks can send bogus routes to the routers, redirecting traffic through their devices, and then decide to forward, discard, or reply to the message. In order to reduce visibility, they may send a route to a target device alone instead of the entire network (Bellovin 1989).

1.5.1.2.2.2 The Defense — The defense for this is a paranoid packet filter, filtering packets with spoofed IP addresses. This, however, cannot be employed for networks that need to hear themselves to retain knowledge of directly connected networks. Authenticating RIP packets is a good defense but difficult to implement for a broadcast protocol unless used with public-key cryptography. This can authenticate immediate senders but not gateways that may be deceived further upstream (Bellovin 1989).

1.5.1.2.3 Exterior Gateway Protocol Attacks

The Exterior Gateway Protocol (EGP) is designed for communication between “exterior gateways” or “core gateways” about autonomous systems (ASs). Data exchanges are usually poll responses with sequence numbers, making it difficult to inject routes (Bellovin 1989).

1.5.1.2.3.1 The Attack — A possible attack is to impersonate an alternate gateway in the same AS. As the core gateway systems are aware of the gateways, this may not work, but if a gateway is down, then attackers can impersonate it (Bellovin 1989).

1.5.1.2.3.2 The Defense — Defense against this attack is the fact that intruders can attack only from existing gateways or hosts that are on the main net and, hence, topological. Sequence number attacks are possible, but the topological restrictions aid in the defense (Bellovin 1989).

1.5.1.2.4 Internet Control Message Protocol

Internet Control Message Protocol (ICMP) as a carrier of network management data in the TCP/IP protocol suite carries data that an attacker would like to get access to. Security holes of this protocol make it vulnerable to attacks (Bellovin 1989).

1.5.1.2.4.1 The Attack — The ICMP redirects messages used to advertise hosts of better routes and can be exploited like the RIP, except that redirect messages are responses within an existing connection and also applicable to a limited topology. ICMP may also be used for targeted DoS attacks using messages like “destination unreachable” and “time to live exceeded.” Sending fraudulent subnet mask reply messages is an attack with a more global impact (Bellovin 1989).

1.5.1.2.4.2 The Defense — The defense against ICMP attacks involves checking and verification of messages to ensure they are relevant to the connection. This checking can handle many issues (less applicable for User Datagram Protocols [UDP]). A possible means of prevention against redirection attack may be to limit route changes to the specified connection only, and subnet mask attacks can be blocked if the reply packets are honored only at an appropriate time (Bellovin 1989).

1.5.1.3 Server Attacks

Many systems handle address-based authentication and trust systems’ vulnerabilities by using authentication servers. The server verifies the authenticity of each client trying to gain access, making it more secure, but it does have some risks (Bellovin 1989).

1.5.1.3.1 The Attacks

If client hosts are not secure, then they may be compromised and, hence, nontrustable. The authentication messages can be compromised using routing table attacks to reroute the messages to other servers/hosts controlled by the attacker(s). If the target host is down, an attacker can send a false reply to authentication requests. A DoS attack can be launched when the fake authentication server replies “no” to all requests (Bellovin 1989).

1.5.1.3.2 The Defense

Authentication servers should make use of secure means of validating each other and not rely on the TCP-based trust authentication. Cryptographic techniques offer better protection (Bellovin 1989).

1.5.1.4 Some Other Services/Protocols

Some of the other services or protocols, though not inherently insecure, can still be susceptible to attacks. A good defense against this is good implementation of services. Some of these are detailed as follows.

1.5.1.4.1 The Finger Service

The finger service gives information about its users, including full names, phone numbers, and so forth, which can be useful data for password crackers (Bellovin 1989). Best practice requires restricting such information to authenticated users only.

1.5.1.4.2 Electronic Mail

Almost all people using the Internet use electronic mail, popularly known as e-mail. This makes a large amount of sensitive and/or personal data open to attack. Traditionally, e-mail servers did not provide authentication, making them susceptible to attacks (Bellovin 1989).

1.5.1.4.2.1 Simple Mail Transfer Protocol — Simple Mail Transfer Protocol (SMTP) is a basic service that allows relay of e-mails, with only eight basic commands, such as HELO, MAIL, RCPT, DATA, and so forth. The most common security threats associated with this are as follows:

- **DoS:** This attack is launched by flooding a computer or network with a very large amount of traffic that legitimate traffic is denied. “Mail bombing” is launched when tens of thousands of e-mails are generated and sent automatically to cause disruption to services (Harris and Hunt 1999).
- **Information gathering:** The simple commands of the SMTP service (like VRFY) may be used to gather information that can be used for hacking attempts. Bugs in application implementation of SMTP have also been known to have led to various exploits (Harris and Hunt 1999).

1.5.1.4.2.2 The Post Office Protocol — The Post Office Protocol (POP) allows remote retrieval of e-mails from central e-mail servers. This system provides authentication using single-line command containing a username and a password. This restricts passwords to the conventional type and is weak (Bellovin 1989). Alternate mechanisms make use of “one-time-passwords,” and newer versions are capable of sending usernames and passwords as two commands (Peng et al. 2007).

1.5.1.4.2.3 PCMAIL — The PCMAIL protocol uses a mechanism similar to POP, but it provides a password change command containing both the old and new passwords in the same (encrypted) line, making it more dangerous (Bellovin 1989).

1.5.1.4.3 File Transfer Protocol

The file transfer protocol (FTP) uses login–password combinations for authentication, which is too simple for adequate security. Many sites now employ one-time-password authentication to overcome this weakness. The optional “anonymous FTP,” enabled in most cases, bypasses the authentication and therefore should not contain any sensitive data (Bellovin 1989; Harris and Hunt 1999).

1.5.1.4.4 Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) is a tool to assist network management and hence needs to be secured, and null authentication should not be used. Even read-only access gives access to sensitive information that can be used to launch other attacks (Bellovin 1989).

1.5.1.4.5 Telnet

Telnet allows simple console access to remote devices, but this makes use of plaintext communications, making it vulnerable to packet sniffers that may gather usernames and passwords.

1.5.1.4.6 Remote Booting

Reverse Address Resolution Protocol (RARP) and Bootstrap Protocol (BOOTP) with Trivial File Transfer Protocol (TFTP) can be used to remote-boot diskless workstations and gateways, which is a tempting target for attackers as they can gain control if they can alter the boot sequence. RARP is weaker as it works over the Ethernet network and hence inherits all its security challenges. BOOTP tries to improve this by adding a 4-byte random transaction ID. The greatest protection is that the attacker has a very small time-frame window as the booting system quickly changes states (Bellovin 1989).

1.5.1.5 Trivial Issues

Some issues are quite trivial, and the chance of occurrence or impact of the occurrence or both is quite small. However, they still deserve mention, as follows.

1.5.1.5.1 Local Network Vulnerabilities

In most cases, the local network is considered as trusted. This opens up issues like “eavesdropping” or Address Resolution Protocol (ARP) attacks to gather reconnaissance or spoofing addresses of key devices (servers). The attacker can cause other issues like broadcast storms for a DoS attack, mandatory access control (MAC) address instabilities by responding to unrelated ARP requests, and so forth (Bellovin 1989).

1.5.1.5.2 TFTP

TFTP allows file transfer without any authentication. All the files on the server are accessible without restriction. Hence, administrators of the system should ensure that the scope of files accessible through TFTP is limited (Bellovin 1989).

1.5.1.5.3 Reserved Ports

The use of the reserved port numbers as a possible authentication on Berkeley-derived systems is a weak and susceptible method. Administrators should not rely on such authentication schemes when communicating with such hosts (Bellovin 1989).

1.5.2 DoS and Distributed DoS

A prominent method of attack that has a history of bringing an entire network to a standstill is called a DoS attack. One of the key challenges is identifying legitimate requests from malicious ones (Peng et al. 2007). The fact that the protocols are not designed to work securely (Bellovin 1989) does not help either.

1.5.2.1 Background

The goal of the Internet was to provide open and scalable networks among defense, education, and research communities in physically closed locations where security was not a major concern. Along with the rapid growth of the Internet and widespread access, attacks also grew, from a mere 6 attacks in 1988 to 137,529 in 2003 (CERT 2006).

1.5.2.2 DoS and Distributed DoS Attacks

DoS attacks are launched by overwhelming the service under attack with bogus requests, exhausting the available limited hardware and/or software resources so that legitimate request to the service is denied. This kind of attack is also called bandwidth attack, targeting CPU capacity or memory of servers and network devices, stack space, and so forth (Peng et al. 2007).

Distributed DoS (DDoS), however, happens in two stages. An attacker first installs his/her tools on a number of compromised systems on the Internet, thereafter called “zombies,” which the attacker can now control. A coordinated attack can then be launched at a preappointed time. Attackers may use anywhere from dozens to hundreds of zombies, distributed geographically, sometimes making use of spoofed IP addresses, making them harder to track (Peng et al. 2007).

In a version of the DoS and DDoS, called the “distributed reflection attack,” an attacker will send a large number of request packets to various servers or hosts with a spoofed source IP address of a target host, causing them to reply to the target host. All the replies funnel down to the target host, creating an amplification effect, often difficult to trace or locate. They can be of very high volume, making any kind of reconnaissance difficult. Current day technology has made it quite trivial to enlist a large army of “zombies” on the internetwork to launch such an attack (Peng et al. 2007). It is even possible to set up such an army at very low costs on the cloud infrastructure (Chen et al. 2010).

1.5.2.2.1 Protocol-Based Bandwidth Attacks

These attacks draw their strength from inherent weakness in the protocol and can be launched effectively from a single source. Some examples of these attacks are as follows.

1.5.2.2.1.1 Sync Flooding — This attack is launched on a three-way handshake mechanism in a TCP connection establishment. In the three-way handshake, a client sends a SYN packet to a server, and the server replies with an acknowledgement (ACK) for the SYN request along with

its own SYN signal, creating half-open connection. The client then responds with an ACK for the SYN from the server, completing the three-way handshake. The attacker floods the server with SYN requests without ACK server responses, causing half-open connections. This makes the connections unavailable to genuine requests, thereby launching a DoS attack (Harris and Hunt 1999; Peng et al. 2007).

1.5.2.2.1.2 ICMP Flood (Smurf Attack) — The ICMP based on the IP protocol is used for diagnosing network status. An example is the Smurf attack, where a ping packet may be sent to a broadcast address with the spoofed source address of a target host directing all the ping replies to a target device, thereby flooding it with very large volume, leading to a DoS attack (Peng et al. 2007).

1.5.2.2.1.3 HTTP Flood — The World Wide Web (www), the most popular application on the net, is a prime target for attacks. It uses the Hypertext Transfer Protocol ([HTTP](http://http)) on port 80. HTTP flood is a type of DoS (or more effectively launched as DDoS) attack where a web server is flooded with more HTTP requests than it can handle. It is almost impossible to distinguish between legitimate and attack traffic, and hence, any kind of defense is difficult (Peng et al. 2007).

1.5.2.2.1.4 Session Initiation Protocol Flood — The Session Initiation Protocol (SIP) is used for VoIP communications. SIP Flooding attacks are easiest to launch, draining resources of both ends of the communication. It can severely affect Quality of Service (QoS) and can lead to DoS (Tang et al. 2012).

1.5.2.2.1.5 Infrastructure Attacks (on the Domain Name System) — The Domain Name System (DNS) helps to resolve friendly domain names to their IP address. This system is susceptible to attacks like DoS, password gathering, and so forth (Bellovin 1989). A combination of DNS and routing protocol attacks is most disastrous, where an attacker replies to all DNS queries and routes the traffic through a subverted host, gaining access to all traffic (Bellovin 1989). Alternatively, DNS can be queried recursively to download the entire name space, which an attacker can use to discover weak spots in the system. DNS authentication schemes are good defenses against such issues (Bellovin 1989). DNS servers are considered high-value targets as attacks can bring down key Internet services that rely on it.

1.5.2.3 DoS and DDoS Attack Defenses

The best practices for DoS and DDoS attack defense generally follow the following steps or stages, applied before, during, or after the attacks.

1.5.2.3.1 Attack Prevention

Prevention tries to stop attacks before they become malign. Coordinated systems working upstream in a network try to identify the attacks (especially spoofed packets) as they are being launched and are filtered closer to the attack sources (Peng et al. 2007).

1.5.2.3.2 Attack Detection

A challenge in this phase is to identify attack traffic from spontaneous bursts of legitimate traffic (flash crowds). An official football portal getting a sudden burst of traffic during a game but bring

relatively quiet otherwise is a good example of this. Statistical approaches using artificial intelligence (AI), looking for traffic anomalies and trends that indicate attacks, are good defenses. Multi-Level Tree for Online Packet Statistics (MULTOPS) (Gil and Poletto 2001) monitors data rate in the uplink and downlink, assuming they will be proportional, and excessive variation (in either direction) indicates an attack (Peng et al. 2007).

1.5.2.3.3 Attack Source Identification

Identifying the source of attack cannot be done at the victim site and requires coordinated effort from participating Internet Service Providers (ISPs) (Peng et al. 2007). One scheme inserts IP traceback information into the packets as they traverse each hop. IP traceback by active insertion, probabilistic packet marking (PPM), probabilistic IP traceback, and hash-based traceback are examples of such schemes. These push elimination of attacks further upstream and are hence more effective (Peng et al. 2007).

1.5.2.3.4 Attack Reaction

Attack reaction needs to be timely and able to differentiate between attack packets and legitimate packets, which becomes most difficult in cases of distributed reflector attacks. In a DoS attack, reaction is more efficient closer to the source and detection is more efficient closer to the destination (Peng et al. 2007). Ingress packet filtering filters all incoming packets from outside the network with internal source IP address ranges, and egress packet filtering filters outgoing packets with an external source IP address. If all gateways employ both, majority of DoS attacks, which are based on spoofed IP addresses, can be prevented (Peng et al. 2007).

Router-based packet filtering takes ingress filtering to the core layer of the Internet, as each link on the core has limited possible source addresses. This filtering is still at a coarse level as the knowledge of the IP addresses is limited within each AS (Peng et al. 2007). The Source Address Validity Enforcement Protocol (SAVE) enables routers to learn valid source addresses and, hence, more effectively block invalid (spoofed) source IP addresses (Peng et al. 2007).

1.5.3 Botnets

High-speed networks available to low-tech users open easy targets for attacks. Attackers find vulnerable hosts with security holes and install “bots” (or “robots”) by executing a code sent to users as e-mail attachments or a browser link that, when clicked on, executes script on the system. This system can be controlled by the attacker. Attackers commonly rely on Internet Relay Chat (IRC) or bot communication. The bots wait on IRC for control instructions from the attacker. This network of bots on the Internet is called a “botnet” (Peng et al. 2007).

Once attackers have a botnet under their control, they can launch different kinds of attacks, DoS type being the most common. Some are even capable of remote updates, allowing the attacker to install patches and add more functionality or design specific targeted attacks using IRC (Peng et al. 2007).

1.5.4 Database, Web, and Cloud Security

In general terms, all computing systems work on data. This section will focus on security aspects relating to three popular areas in internetworked computing, namely, database security, web security, and security in the relatively new infrastructure, the cloud.

1.5.4.1 Database Security

Applications work on data, which may be in very large volumes, and may be organized into well-ordered collections and managed using database management systems. Attacks against this are common, mainly for financial gain.

1.5.4.1.1 Background

With the rise of computing and database systems as key technology for management and decision making, misuse, attacks, and damages to this can lead to heavy losses. Attacks against this kind of system can be categorized into *unauthorized data observation*, *incorrect data modification*, and *data unavailability*. Good security would involve three tasks: (1) *identification and authentication*, where systems identify the users and verify their ID; (2) *access control*, where users are given controlled access to and only to the resources for which they have authorization; and (3) *encryption*, to protect the data in storage and as they travel over the network. Database security is concerned about data in a database and mostly addresses the second element, access control (Jajodia 1996).

1.5.4.1.2 Access Control for Databases

When users try to access a data object, they are verified against their authorizations, and access is granted to authorized users. Digital signatures help to ensure data integrity and also to verify the source (Bertino and Sandhu 2005). Availability can be improved by strengthening against different kinds of DoS attacks, discussed elsewhere in this chapter.

1.5.4.1.2.1 Discretionary and Mandatory Access Control Policies — The early development of database access control focused on two models, the *discretionary access control (DAC) policy* and the *MAC policy* (Bertino and Sandhu 2005; Jajodia 1996). DAC uses policies that allow subjects to grant access to data to other subjects (Bertino and Sandhu 2005; Gollmann 2010), creating a flexible system that has been adopted by many commercial systems and applications. DAC for relational databases introduced decentralized authorization administration and commands for revoking and granting of authorizations, negative authorizations, role-based and task-based authorizations, temporal authorizations, and context-aware authorizations (Bertino and Sandhu 2005).

The weakness of the DAC model is that it does not have control on data in transit. This can be capitalized on by Trojans and other malicious programs by using *covert channel leaks* (a protocol or feature that is used to hide data within normal communications) and sending out data undetected (Bertino and Sandhu 2005; Bertino et al. 1995). MAC tries to address these issues using a model based on information classification, in which subjects are given access to objects (passive entities storing data) based on classification labels, forming partially ordered sets (Gollmann 2010), and access is granted only if some relationship is satisfied between subjects and objects (Bertino and Sandhu 2005; Jajodia 1996; Bertino et al. 1995; Bertino 1998).

1.5.4.1.3 Additional Areas in Context

As databases became more advanced, the contexts of applications represented in databases became richer with semantic models, hierarchies, stored procedures, and so forth, generally and collectively called “schema,” which needs to be protected as well. The new challenge with newer multimedia content in databases meant that automatic interpretation of the contents was not possible

for them, and hence, both the DAC and MAC had to be extended to cater to this (Bertino and Sandhu 2005). The context of Digital Rights Management (DRM) is similar to copyrights and is more legal (Gollmann 2010) than technical; hence, it is not discussed in this chapter.

Data security challenges are evolving from the traditional concepts of *confidentiality*, *integrity*, and *availability* to *data quality*, *timeliness*, *completeness*, and *provenance* (Bertino and Sandhu 2005). We need to assess and verify the database in terms of quality and performance along with security and access control.

1.5.4.2 Web Security

The far-reaching connectivity of the web technology has brought with it not only huge possibilities but also far-reaching security challenges. In light of the awareness of the risks and not-so-few attacks with more-than-trivial impact on the systems, vendors and researchers have been working towards adding security into the services offered to make them more *stable*, *reliable*, and *available* (Rubin and De Geer 1998).

1.5.4.2.1 Server Security

The web technologies work on the client–server model, where browsers (clients) access content on a central server, and hence, the server is the central point of attacks (Rubin and De Geer 1998). Some of the issues based on the Unix-based Apache server (as an example) are discussed. Though there are variations in server installations, the common discussion is applicable (Rubin and De Geer 1998).

1.5.4.2.1.1 Basic Configuration — The web server configuration file in the root directory contains directives that control files containing usernames, passwords, access control information for the files in the document tree, default permissions, local overrides, and so forth, providing the basic configuration for the website. These, if incorrectly configured, can open security vulnerabilities (Rubin and De Geer 1998).

1.5.4.2.1.2 Setting Up a Root — The most common error an administrator makes is to run the web server as a root. This allows root access to the web server and can grant access to the privileged port. The best-practice alternative is to create a user privilege for the web server with appropriate access. The application can then provide individual user-level access based on usernames and passwords (Rubin and De Geer 1998).

1.5.4.2.1.3 Local Control Issues — The server-side executable code allows dynamic values like current date and time to be inserted into web pages. This can open potential security holes. A best practice is to disable execution of commands on servers and also disable the ability of subdirectories to override default behavior (Rubin and De Geer 1998).

1.5.4.2.1.4 Authentication — Since web services depend on name services, security based solely on name services can be compromised if an attacker gains control over the name service. Methods like authentication, combining IP address or digest authentication, and using challenge–response with MD5 hash messages are much stronger than username–password–based authentication. The public-key infrastructure is the best-known scheme for authentication of client and server, though this is common for servers and not for clients. FTP allows anonymous access, which is another

potential risk, and care should be taken that the FTP upload area does not spread over to the HTTP area (Rubin and De Geer 1998).

1.5.4.2.1.5 Scripting — Servers can execute scripts (programs that can respond to calls with arguments) to process active content. Common Gateway Interface (CGI) is a middleware for interoperability of active content. Some of the attacks are launched by loading the calls with parameters that the script cannot handle. A clear verification of data helps to subvert these kinds of attacks (Rubin and De Geer 1998).

1.5.4.2.2 Securing the Host

The web server is compromised if the host computer on which this is installed is compromised. Therefore, it is relevant to consider aspects of host security for web server security.

1.5.4.2.2.1 Basic Threats — Trusted systems that establish trust to substitute formal proof of security are of no use in the web. Root privilege access must be safeguarded from attacks. The webmaster must insist on accountability of each content, checking authorization for every transaction and auditing the system regularly, more frequently if changes are frequent (Rubin and De Geer 1998).

1.5.4.2.2.2 Notification and Recovery — Notification services and event logs are important tools for timely response to events. Since we expect system breakdown, recovery should also be planned, starting with a checklist of high-availability websites, common issues on data centers, and so forth, as well as other steps for intrusion handling (Rubin and De Geer 1998).

1.5.4.2.3 Securing Data Transport

Security of data as they travel over the internetwork between the source and the destination is susceptible to various kinds of attacks. The network-layer approach encrypts the data at the network layer, transparent to the application layer. The application-layer approach works at the application layer, and encrypted data are passed to the network layer for transmission. The application-layer approach is better suited for web as it is easier to define trust boundaries between transacting agencies (Rubin and De Geer 1998).

1.5.4.2.3.1 Secure Socket Layer — The most common application-layer security mechanism is the stream-based protocol, Secure Socket Layer (SSL) (Rubin and De Geer 1998).

The client and server exchange handshake messages to establish communication parameters, including protocol version, encryption algorithms, exchange keys, and so forth, and authentication certificates. The data mode ensues, encrypting all messages from applications, where SSL becomes a ubiquitous layer providing encryption for [HTTP](#), e-mail database access, and so forth (Rubin and De Geer 1998). SSL works at the transport layer (Gollmann 2010).

The initial versions of SSL did not include client-side authentication. In addition, they had many flaws, including protocol flaws and random number generation for encryption. The 40-bit key used by Netscape Navigator was broken by brute force attacks, creating doubt about security capability (Rubin and De Geer 1998).

1.5.4.2.3.2 Security and Export Controls — The US export control laws categorize strong encryption as a weapon and control its use internationally. Internet communications transcend geographic boundaries, and governmental restrictions make it harder to get vendors to agree and comply with improved security standards (Rubin and De Geer 1998).

1.5.4.2.4 Mobile Code Security

Mobile code refers to general-purpose scripts that run in remote locations, opening a world of possibilities for devices connected to the Internet. A general-purpose interpreter as part of a browser is often buggy and can allow attackers to exploit it. Sandboxing, code-signaling, and firewalling attempt to minimize issues in this arena. “Proof-carrying code” is a newer area, in which the mobile programs carry proof that certain properties are satisfied (Rubin and De Geer 1998).

1.5.4.2.5 Anonymity and Privacy

User activity on the web is logged more, recorded more, analyzed more, and disseminated more as use increases, increasing the risk of exposure of privacy. This may be collected and analyzed by advertising companies who build massive databases of user data to conduct targeted advertising (Rubin and De Geer 1998).

Technological attempts to protect against this kind of risk include *mixes*, *proxy mechanisms*, and *crowds*. Mixes create anonymity by forming a mix network as a relay point, removing original source information. The proxy between the client and server removes the source information and hides individual user information by attributing each activity to the crowd. The crowd is a more effective method for ensuring anonymity (Rubin and De Geer 1998).

1.5.4.3 Cloud Computing and Security

Computing systems evolved from being completely centralized on mainframes, to decentralized personal computers, to client–server models, and back to the centralized access concept with cloud computing. Cloud computing takes the advantage of the extreme low-cost cloud infrastructure and the availability of high-speed Internet to remove resource-intensive tasks from user devices. As personal and business information and systems migrate to the cloud, a “sweet pot” for attacks (Chen et al. 2010) is created.

1.5.4.3.1 Not Everything Is New

As there are many arguable boundaries of what defines the term “cloud,” we will consider cloud computing security under *software as a service (SAAS)*, *platform as a service (PAAS)*, and *infrastructure as a service (IAAS)*, providing users with on-demand service, broad network access, resource pooling, metered service, and so forth on virtually infinite hardware resources available on a pay-per-service-use basis (Chen et al. 2010).

The concept of security on the cloud is not necessarily new as it is similar to traditional applications and web hosting. Cloud security therefore can be seen as an extension of web security, data outsourcing, and virtual machine security (Chen et al. 2010; Subashini and Kavitha 2011). The area of web security is discussed in Section 1.5.4.2.

1.5.4.3.2 Something Is New

The cloud offers a potential alternative to botnets, at a small cost, with a more trustworthy source, though easier to shut down than traditional botnets. Shared information may be accessible through side channels, covert channels, and so forth, exploiting possible bad or weak administration oversights or loopholes. Another new issue is reputation-fate sharing, where a large fraction of legitimate IP addresses may be blacklisted due to one spammer in the ecosystem. Activity patterns on the cloud may be visible to other applications on shared resources, side channels, and covert channels, opening it to reverse-engineering attacks to reconstruct customer data. Users also need to accept longer trust chains and may be faced with attackers posing as a provider or a provider selling off his/her service to the highest bidder as a business decision (Chen et al. 2010).

The virtual machine environments may be more secure than the Operating System (OS) by providing a “sandbox” environment where the system is compromised only when the virtual machine and the host OS are compromised (Chen et al. 2010).

1.5.4.3.3 The Cloud Way

The cloud provider should hence be geared up to provide multiple security levels, catering to the varying user requirements. The provider’s security expertise can focus on strengthening this, and users can focus on the application. Further research is required to identify possibilities and impact of different threats coexisting on the same shared infrastructure, launching coordinated attacks (Chen et al. 2010; Subashini and Kavitha 2011).

1.5.5 *Mobile and Wireless (Including Android and Smart Devices)*

Mobile phones with a fully fledged OS have risen about 200% from Q3/2009 to Q3/2010 (Becher et al. 2011). A vast majority of users of these are relatively low-tech and non-computer savvy and are easy targets for attackers. It is interesting to note that all the speculations about possible security issues on mobile platforms are yet to materialize, probably because of the lessons learned from desktop security and awareness of plausible attack scenarios (Becher et al. 2011).

1.5.5.1 *About Mobile Security: Definition and Need*

This section discusses security on portable or mobile devices, including smartphones, tablet PCs, and any such device in the category. The possible areas of interest for an attacker are as follows (Becher et al. 2011):

- *Creation of costs*: Billed events that use the network service provider’s services, or payment systems that use mobile systems as a trustworthy channel or mobile devices as payment authentication using near field communication (NFC).
- *Firmware update*: Facility to update its firmware, providing additional features, or for patching any bugs in the current version and *remote device management* capability, where some features or the entire device can be managed from remote PCs.
- *Limited device resources*: Mobile devices are of limited form factor, limited power in terms of CPU, RAM, battery, and so forth.

- *Expensive wireless link*: The wireless link is expensive in monetary communication costs as well as computation costs, consuming the very limited resources on devices.
- *Reputation*: The mobile operator is able to track every communication event generated from the device as initiated by the user and hence charged to the user, even if generated by third-party applications.

1.5.5.2 Categories of Attacks on Mobile Devices

Attacks on mobile devices may be classified under the following categories based on their nature.

1.5.5.2.1 Hardware-Centric Attack

User data may be compromised by forensic analysis, but this can be launched only with physical access to the device and hence is not easily exploitable on a large scale (Becher et al. 2011).

- Intercepting communication between a mobile network operator (MNO) and a device in *man-in-the-middle* (MITM) attacks, either for eavesdropping or injecting messages into the communication (Becher et al. 2011).
- *Device attacks* include exploiting the features of Joint Test Action Group (JTAG) hooks accessible in production devices or forensic analysis of the devices. The JTAG issue can be addressed by enforcing industry requirements on production devices and the latter by encrypting personalized data (Becher et al. 2011).

1.5.5.2.2 Device-Independent Attack

Device-independent attacks do not exploit the weaknesses of devices. Eavesdropping on the wireless connection, leaking mirrored data from the devices or back-end systems, and violating confidentiality of the stored data are some examples of this kind of attack (Becher et al. 2011).

- Global system for mobile communications, originally Groupe Spécial Mobile (GSM), employs cryptography to protect individual communications as it uses shared media (air links). A subscriber identification module (SIM) card contains the unique subscriber ID, keys, and algorithms used for the encryption. It uses symmetric cryptography to authenticate a mobile device against the base station to prevent fraud, such as impersonation attacks, eavesdropping, etc. This method does not address jamming of the frequency channel as other layers implement methods like frequency hopping to counter this (Becher et al. 2011).

Encryption algorithms can now be broken in seconds with the growth of computational power. Another weakness is that GSM encrypts the encoded signal instead of encrypting the message and then encoding, giving sufficient redundancy for cryptanalysis to break the encoding key (Becher et al. 2011).

- Bluetooth as a cable-replacement alternative for communication has been open to exploits. When unsuspecting users bypass security standards and leave Bluetooth open, it opens possibilities for attacks. Attackers force devices to reveal their identity in what is called the neighbor discovery attack (Khatri et al. 2009).

- It is now possible to set up a rogue base station called international mobile subscriber identity (IMSI) catcher with cheap hardware and open-source software, allowing attackers to exploit unsuspecting users. The radio access mechanism opens the devices to attackers in the vicinity, as they impersonate a legitimate device establishing communication with the devices, known as “evil twin” (Becher et al. 2011).
- Short messaging service (SMS) infrastructure flaws arose as the MNOs allowed the sending of SMS from the Internet for additional revenue, making it possible for a user with a PC with broadband Internet to deny voice service to an entire city by overwhelming the network with SMS (Becher et al. 2011).
- Multimedia messaging service (MMS) exploits users by first sending a forged MMS message directing them to a false server. The server discovers the IP address of the device and sends UDP packets to the device at periodic intervals, preventing the device from reaching standby mode (sleep deprivation attack) (Khatri et al. 2009), exhausting the batteries about 22 times faster. If attackers can predict the range of addresses of a service provider, they can launch the attack without users responding to MMS and unaware to the user as well (Becher et al. 2011).
- Universal Mobile Telecommunications Systems (UMTSs) address most of the issues of GSM. UMTS improves the encryption and authentication of mobile systems and prevents rogue station attacks. UMTS still suffers from issues like clear text IMSI, allowing eavesdropping and “evil twin” issues. DoS attacks are possible on UMTS (or 4G) using well-timed low-volume signaling or by jamming the presence service (Becher et al. 2011).
- The attacks can be towards back-end systems when media data are stored on the MNO with only a password. This can be attacked using web vulnerability, with which the attacker can reset the access password and gain access to data. Attacks against the home location register (HLR) are shown to be capable of reducing legitimate traffic by up to 93%. Attacks against user data on the cloud accessed by mobile devices are discussed Section 1.5.4.3 (Becher et al. 2011).

1.5.5.2.3 Software-Centric Attacks

This is the most common type of attack, often based on technical vulnerabilities leading to security violations. The highly insecure mobile web browsers often make it an easy target for attackers (Becher et al. 2011).

- *Malware* deployed on a device can be used for information or identity theft, espionage, and so forth by collecting behavioral data including GPS locations, e-mails, and so forth. This may be sent out using cryptographic and/or stealth techniques, making it harder to detect. *Eavesdropping*, *financial attacks*, *mobile botnets*, and *DoS attacks* can result from this.
- *SMS vulnerabilities* including bugs in an SMS parser can result in DoS attacks. This was fixed later by firmware updates. MMS vulnerabilities allow dissemination of malware to unsuspecting users.
- *Mobile web browsers* have emerged from pure web browsing to running full-fledged applications. Clicking a hyperlink to make calls is an example of features that can be an attack target.
- *Operating systems* protected by active steps like limited privileges and process isolation, hardened kernels, sufficiently secure default settings, timely updates, software capability attestation, and so forth can help to improve device security.

- *The limited Graphical User Interface (GUI)* not able to display the string that the system intends to and malware capable of capturing user sequences and replay it are examples of attacks exploiting GUI limitations, for which Turing tests (CAPTCHA) defense is effective.

1.5.5.2.4 User-Layer Attacks

These attacks target the mobile user with nontechnical approaches. Most of the attacks in today's computing ecosystem are not necessarily technical; they mislead users to override existing security systems.

Attackers may be passive, not altering the contents or working of the system. Active attackers come between the user's interaction with the systems changing data and/or the workflow (Becher et al. 2011). The following may be the goals of the attacks.

- *Eavesdropping*, intercepting an ongoing communication
- *Availability attacks* like jamming communication channels making services unavailable
- *Privacy attacks* locating and tracking user patterns
- *Impersonation attacks* trying to impersonate another user or device to obtain access fraudulently

1.5.6 Social Media and Social Aspects of Computer Security

Social aspects of computer security involve security relating to the recently growing social networking applications on web and mobile platforms as well as the social element of security. Social media sites and/or servers hold a very large number of users and their personal data, which need safeguarding from exploits, while providing access to it to its intended audience. Issues include unsolicited messages (spam), stealing private data, identity theft, impersonation, and so forth. In reverse social engineering attacks, a victim is tricked into initiating contact with an attacker, who builds up trust and uses it for various kinds of fraud, mostly financial. Some of the attacks make use of features of the social networking sites to launch these attacks (Irani et al. 2011).

Securing computing system can now be automated, but that does not solve the issue. The last link in computer security, users, can be manipulated or tricked into security breaches. Attackers circumvent the technical security by appealing to the victim's emotions like fear or excitement or building up trust with the victim and manipulating it to extract information (Workman 2007).

Attacks include *spamming* (sending unsolicited bulk e-mails), *phishing* (trying to draw sensitive information from victims posing as a legitimate party), *identity theft* (assuming the identity of another and misrepresenting it to take advantage of trust relations that may have existed), and *financial fraud* (establishing trust or making a claim like having won the lottery and getting the users to transfer funds into the attacker's account or selling nonexistent articles online), just to name a few. Theories behind how and why these kinds of attacks are successful are to be discussed in a nontechnical, psychological, or behavioral perspective and are hence beyond the scope of this chapter.

1.5.7 Multimedia Security

Digital content grew beyond text and documents as multimedia became available in the digital format. The evolution and widespread availability of high-speed Internet have led to the growth of multimedia services over the Internet. Services like TV pay channels; copyright contents including

images, audio, and video; IP-based conference calls and video conversations; VoIP; and so forth need to be secure to ensure confidentiality, integrity, and availability.

1.5.7.1 Special Features of Multimedia

Some special features of multimedia, differentiating them from text, are bulky size, inability to perform lossless compression in some applications (like medical imaging), cost of encryption, presence of high redundancy (causing block ciphers to leave patterns in the cipher output), loss of avalanche property, and catering to the needs of diverse multimedia applications. Some special features of video and images include *format awareness*, *scalability*, *perceptibility*, and *error tolerability* (Furht and Kirovski 2005).

1.5.7.2 Encryption in Multimedia

Selective encryption for digital images was adopted for a trade-off between encryption load and security. It was later shown that encryption of some significant bits alone was insufficient, especially for MPEG video. As there is not much difference between video and images, most image encryption techniques can be extended to video encryption, and most MPEG encryption methods can be applied for image encryption directly, as employed by *joint image/video encryption*. The MPEG encryption encrypts selective macro blocks. Other methods for video encryption algorithms (VEAs) divided the video stream into 128-byte odd and even streams and XORed for at least 50% more efficiency. A method that performs secret linear transform on each pixel, which is a method combining stream and block ciphers, which attains better trade-off between speed and security, was also proposed. In a different and definite advancement, we saw the application of 1-D, 2-D, and 3-D chaos maps in images or digital frames for *chaos-based image/video encryption*. The Chaotic Video Encryption Scheme (CVES) is a chaos-based encryption scheme using multiple chaotic systems (Furht and Kirovski 2005).

Though many systems are proposed or in use for multimedia encryption, some are either too weak or too slow. The chaos-based encryption schemes are promising and are under research and development (Furht and Kirovski 2005).

1.6 Defenses in Secure Computing

The sections discussed prior also present defenses against known vulnerabilities. This section will therefore explore some popular defenses, best practices, or models. The best defense seen in the area of computer security is cryptography, which denies data to unauthenticated users. The use of encryption has seen rapid increase in use, from storage to transmission.

1.6.1 Security Policy, Model Architectures, and so Forth

1.6.1.1 Defense In-Depth Model

The defense in-depth model approach applies countermeasures at every layer of the computer network, namely, *data*, *application*, *host*, *network*, *perimeter security*, and *physical security*. *People*, *policies*, and *procedures* form the overarching layer because it affects every other layer in consideration (Figure 1.2).

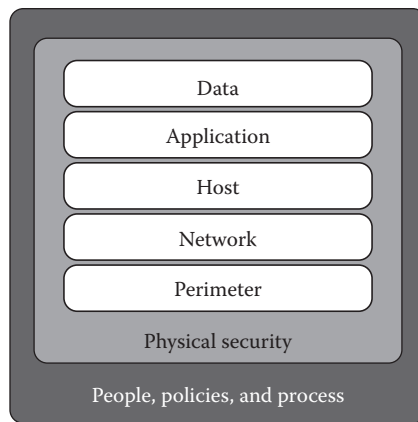


Figure 1.2 Defense in-depth model.

Data security considers protecting data in storage and access, whereas *application security* addresses securing the applications with good coding practices, timely patches, and bug fixes. *Host security* discusses securing the host platform, OS, and so forth, and *network security* addresses communication over the network. *Perimeter security* addresses securing the perimeter, which is the boundary beyond which the internal network administrator has no more control. *Physical security* ensures that the computing hardware is under lock and surveillance. Over all of these, the *people* who access the systems follow *processes and policies* to access systems (Microsoft Security Content Overview).

1.6.1.2 Access Control Models

Access control is identified as the most important concept for data security. *DAC* and *MAC* models were discussed in Section 1.5.4.1.

1.6.2 Cryptography and Steganography

Cryptography encrypts data as means of securing the channel of communication between the end points. Services like SSL, digital certificates, [HTTPs](#), IPSec, and so forth all work on cryptography (Gollmann 2010). However, encryption is costly in terms of resources, time, speed, and computational and administrative complexity (Bellovin 1989). Steganography hides data in images, making the presence of the data unknown as well.

1.6.3 Firewalls

Firewalls work on the perimeter devices offering filtering of packets traveling in and out of the network. Packet filtering works by selectively allowing or disallowing packets based on some protocols, key words, or rules. Stateful packet filtering keeps track of the state of a communication and hence is more efficient. Proxies go an additional level by acting in the middle in order to sanitize all packets in communication (Gollmann 2010).

1.6.4 Intrusion Detection Systems

Intrusion detection systems (IDSs) monitor network traffic or log files to look for preknown attack patterns (*knowledge-based*) or traffic anomalies (*anomaly-based*). The anomaly-based approach can respond to unknown or first-time attacks, also called zero-day exploits. While context-aware IDSs suppress irrelevant alarms, honeypot systems attract and detect attack traffic (Gollmann 2010).

1.6.5 People, Policies, Procedures, and Practices

Computer security starts from the policies and practices that regulate access for people (Gollmann 2010). All technological solutions eventually funnel down to the people using them and the skills they possess. A survey reveals that 85% of organizations experience recruitment problems because of a lack of adequate cyber security skills or knowledge. In terms of available learning, we have an assortment of “patchwork courses” and a plethora of certifications in the absence of industry standardizations, which does not offer too much help to the people involved (Caldwell 2013).

1.7 Summary and Conclusion

The Internet was not designed to the size and scale we see today. It therefore came with a number of inherent flaws too, which led to numerous kinds of attacks, some of them leading to huge losses, not limited to financial ones. Much advancement has been implemented in the form of authentication and cryptography, forming the key pillars for security to ensure the provision of *confidentiality, integrity, and availability*. The varying needs of a user base make it evident that one solution for all does not suffice, and hence, we have seen research progress in different directions, based on the domain and nature of the resources.

New offerings and future developments like IP version 6 or the mobile applications are designed with sound security best practices in view and hence are expected to be a lot harder to attack. Systems like Multix, designed with ground-up security, will be a lot more resilient to issues (Chen et al. 2010). Consolidation of expertise as in the cloud infrastructure can also be helpful in pooling resources for excellent security at a much lower cost. However, with all the security systems in place, the users, the last link, need to be aware of issues pertaining to their scope of use in order that they are sufficiently aware to safeguard themselves from social engineering types of attacks.

References

- Becher, M., Freiling, F. C., Hoffmann, J., Holz, T., Uellenbeck, S., and Wolf, C. (2011, May). Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices. In *Security and Privacy (SP), 2011 IEEE Symposium on* (pp. 96–111). IEEE.
- Bellovin, S. M. (1989). Security problems in the TCP/IP protocol suite. *ACM SIGCOMM Computer Communication Review*, 19(2), 32–48.
- Bertino, E. (1998). Data security. *Data and Knowledge Engineering*, 25(1), 199–216.
- Bertino, E., and Sandhu, R. (2005). Database security-concepts, approaches, and challenges. *Dependable and Secure Computing, IEEE Transactions on*, 2(1), 2–19.
- Bertino, E., Jajodia, S., and Samarati, P. (1995). Database security: Research and practice. *Information Systems*, 20(7), 537–556.
- Caldwell, T. (2013). Plugging the cyber-security skills gap. *Computer Fraud and Security*, 2013(7), 5–10.

- CERT. (2006). CERT/CC statistics. Available at <http://www.cert.org/stats/certstats.html>.
- Chen, Y., Paxson, V., and Katz, R. H. (2010). What's new about cloud computing security. *University of California, Berkeley Report No. UCB/EECS-2010-5 January, 20(2010)*, 2010–2015.
- Furht, B., and Kirovski, D. (2005). *Multimedia Security Handbook* (Vol. 158). New York: CRC Press.
- Gil, T. M., and Poletto, M. (2001, August). MULTOPS: A data-structure for bandwidth attack detection. In *USENIX Security Symposium*, Washington.
- Gollmann, D. (2010). Computer security. *Wiley Interdisciplinary Reviews: Computational Statistics*, 2(5), 544–554.
- Harris, B., and Hunt, R. (1999). TCP/IP security threats and attack methods. *Computer Communications*, 22(10), 885–897.
- Irani, D., Balduzzi, M., Balzarotti, D., Kirda, E., and Pu, C. (2011). Reverse social engineering attacks in online social networks. In *Detection of Intrusions and Malware, and Vulnerability Assessment* (pp. 55–74). Berlin Heidelberg: Springer.
- Jajodia, S. (1996). Database security and privacy. *ACM Computing Surveys (CSUR)*, 28(1), 129–131.
- Khatri, P., Bhadoria, S., and Narwariya, M. (2009). A Survey on Security issues in Mobile ADHOC networks. *TECHNIA—International Journal of Computing Science and Communication Technologies*, 2(1).
- Microsoft Technet online library. Security Content Overview. Microsoft, n.d. Web. 15 Aug. 2013. Available at <http://technet.microsoft.com/en-us/library/cc767969.aspx>.
- Morris, R. T. (1985). A weakness in the 4.2 BSD UNIX TCP/IP software. AT&T Bell Labs. Technical Report 117, February.
- Peng, T., Leckie, C., and Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, 39(1), 3.
- Rubin, A. D., and De Geer, J. (1998). A survey of web security. *Computer*, 31(9), 34–41.
- Smith, R., Grabosky, P., and Urbas, G. (2004). Cyber criminals on trial. *Criminal Justice Matters*, 58(1), 22–23.
- Subashini, S., and Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network and Computer Applications*, 34(1), 1–11.
- Tang, J., Cheng, Y., and Hao, Y. (2012, March). Detection and prevention of SIP flooding attacks in voice over IP networks. In *INFOCOM, 2012 Proceedings IEEE* (pp. 1161–1169). IEEE.
- Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. *Information Systems Security*, 16(6), 315–331.

