Chapter 1
Computer Security

Jeffrey L. Duffany

1.1 Introduction

Computer security can be viewed as a set of mechanisms that protect computer systems from unauthorized access, theft, damage and disruption of the services they provide. It includes protection from both internal and external threats. Internal threats can be flaws in a software program or operating system. External threats are unauthorized access or human error. Much of computer security is based on the principle of separation which states that one thing cannot affect another if they are suitably separated [1]. The main mechanisms for achieving separation are physical, temporal, logical and cryptographic [1]. Each of these four basic techniques is in widespread use today and security by separation is one of the fundamental principles of computer security. From an implementation standpoint, however, computer security is usually attained by a suitable set of mechanisms to provide confidentiality, integrity and availability of systems and data [1, 2] (see Fig. 1.1).

1.1.1 Confidentiality

Confidentiality is the principle that information is not disclosed unless intended [1]. One of the primary techniques to achieve confidentiality is through the use of cryptography [2]. Cryptographic techniques involve scrambling information so it becomes unreadable by anyone who does not possess the encryption key. For

J.L. Duffany (✉)
Universidad del Turabo, Gurabo, Puerto Rico
e-mail: jeduffany@suagm.edu

K. Daimi (ed.), *Computer and Network Security Essentials*,
DOI 10.1007/978-3-319-58424-9_1

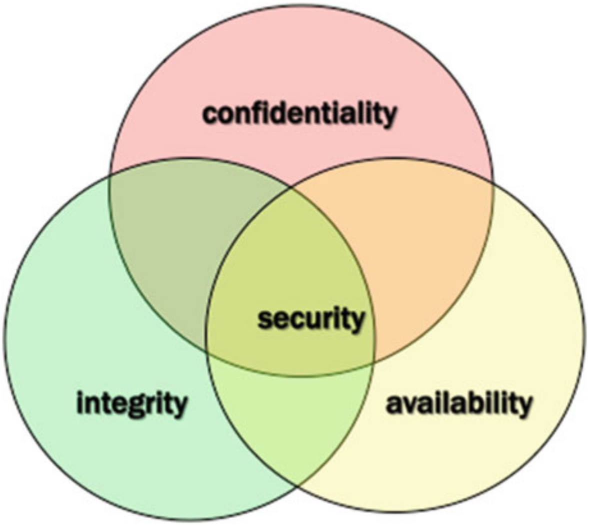


Fig. 1.1 Security at the intersection of confidentiality, integrity and availability

example, hard drives can be encrypted so that information is not compromised in the event of theft or loss. Trusted parties who possess the encryption key can decipher the encrypted data while others cannot.

1.1.2 Integrity

Integrity is assuring the accuracy and completeness of data over its entire life cycle. This means that data cannot be modified in an unauthorized or undetected manner. The mechanism to ensure integrity often involves the use of a hash function, a one-way mathematical function that provides a digital signature of the data to be protected [2].

1.1.3 Availability

For any information system to serve its purpose the stored data must be available when it is needed [1]. High availability systems are designed to remain available at all times avoiding service disruptions due to power outages, hardware failures and system upgrades. Ensuring availability also includes the ability to handle denial-of-service attacks which send a flood of messages to a target system in an attempt to shut it down or block access [1].

1.1.4 Vulnerabilities and Attacks

A vulnerability is a system susceptibility or flaw in the design of the hardware or software and can be exploited to gain unauthorized access. A desktop computer faces different threats as compared to a computer system used in a government or military network. Desktop computers and laptops are commonly infected with malware designed to steal passwords or financial account information or to construct a botnet [1]. Smart phones, tablet computers and other mobile devices have also become targets. Many of these mobile devices have cameras, microphones and Global Positioning System (GPS) information which could potentially be exploited. Some kind of application security is provided on most mobile devices. However, applications of unknown or untrusted origin could result in a security compromise as a malicious attacker could embed malware into applications or games such as Angry Birds.

Government and military networks and large corporations are also common targets of attack. A recent report has provided evidence that governments of other countries may be behind at least some of these attacks [3]. Software and communication protocols such as Supervisory Control and Data Acquisition (SCADA) [4] are used by many utilities including the power grid and other types of critical infrastructure such as the water distribution system. Web sites that store credit card numbers and bank account information are targets because of the potential for using the information to make purchases or transfer funds. Credit card numbers can also be sold on the black market thereby transferring the risk of using them to others. In-store payment systems and ATMs have been exploited in order to obtain Personal Identification Numbers (PINs), credit card numbers and user account information.

1.2 Historical Background

Computing as we know it today had its origins in the late 1930s and 1940s during World War II when computers were developed by England and the United States to break the German Enigma cipher [2]. However computers did not find widespread government, commercial and military use in the United States until the decade of the 1960s. At that time the threatspace was rather limited and the emphasis was on functionality and getting things to work. Computing in the 1960s was carried out using large mainframe computers where users had to share the same memory space at the same time which leads to computer security issues. One program could affect another although this could be intentional or unintentional. This leads to the principle of separation as a primary means of implementing security. Physical separation was not always practical because of the expense, however, temporal and logical separation was widely employed in early mainframe computers even though it leads to somewhat inefficient use of resources. Temporal separation required programs to run sequentially while logical separation was used to give a virtual machine address space to each program.

The 1970s saw the migration toward smaller more affordable minicomputers and the rise of the Unix operating system. One minicomputer cost only a small fraction of what it cost to purchase and maintain a mainframe computer and could support dozens of users. These systems were highly scalable simply by adding more machines connected by networking equipment. Individual machines were often given fanciful names such as harpo, zeppo, chico, (the Marx brothers) or precious stones (diamond, emerald, etc.). Each user had one or more accounts on one or more machines and after logging on to their account were given a command line interface very similar to the Linux systems of today. Basic networking and electronic mail was supported. Each file or folder was given a set of read, write and execute (rwx) permissions to the owner and other users designated by the owner. Toward the end of the 1970s the first personal computers began to emerge from companies such as Apple and IBM.

The 1980s continued the revolution of the personal computer first beginning with the desktop and then laptop computers. Personal computers in the early 1980s typically had hard drives in the range of 40 MB, 64 K of RAM, 8 bit processors and command line user interfaces. As the command line interface was boring to many people one of the main uses of personal computers at that time was video games such as Space Invaders and PacMan (Fig. 1.2). Laptop computers were relatively expensive in the 1980s and became a prime target for theft. The first computer viruses (Fig. 1.3) also began emerging during the 1980s [5]. Floppy disks were used to boot and to share files. The first cybercrimes started making their way into the courtroom and as a result the Computer Fraud and Abuse Act (CFAA) (1984) was passed [1]. On 2 November 1988 Robert Morris released the first computer worm onto the internet and was subsequently found guilty of violating the new CFAA-related statutes [1]. During the mid-1980s Microsoft started developing the NTFS as a replacement for the outdated and severely limited File Allocation Table (FAT) filing system. The US Government issued the TCSEC Trusted Computer System Evaluation Criteria as a means of letting vendors know what they needed to do to make their operating systems more secure [1, 6]. Early adopters started subscribing to online services such as AOL and Compuserve which gave them access to electronic mail, chatrooms and bulletin boards. A member of the Chaos Computer Club in Germany accessed several US government military computer networks [7].

By the 1990s many companies had provided their employees with desktop or laptop computers running the latest version of Microsoft Windows. Many individuals owned their own desktop or laptop computers which were continuously adding new technological features while steadily reducing in price. The 1990s also saw the meteoric rise of the internet and web browsers. E-commerce was enabled by web browsers that supported secure connections such as Netscape [2]. Computer viruses continued to wreak havoc (Fig. 1.3) and the early 1990s saw the rise of many individual antivirus companies that were bought out by their rivals

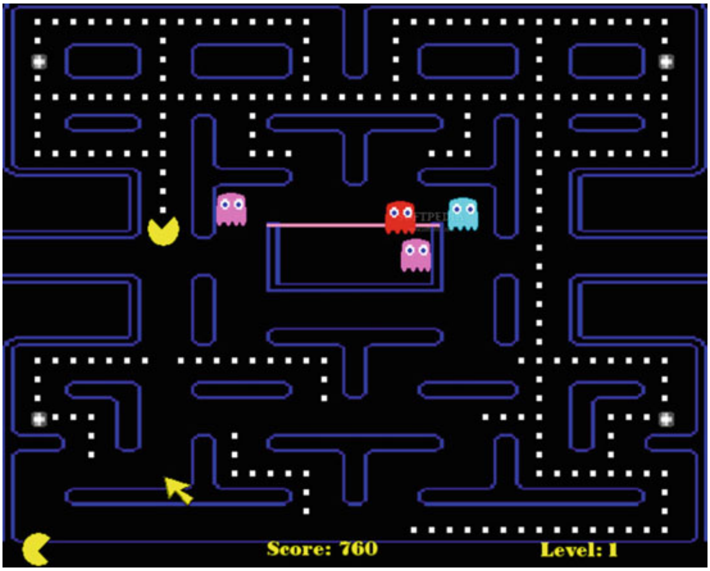
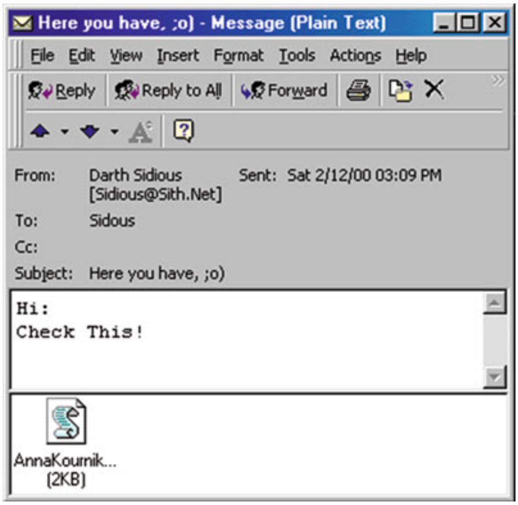


Fig. 1.2 PacMan game screen capture from early 1980s personal computer

consolidating down to a few major competitors. Cellular phones started becoming more affordable to the masses. The Data Encryption Standard (DES) [8] was broken by the Electronic Frontier Foundation [9]. Meanwhile wireless networks and the Wired Equivalent Privacy (WEP) standard emerged that used RC4 stream coding [10]. The Digital Millennium Copyright Act anticipated the potential abuse of copying information in digital form [1].

The decade of 2000 saw increasingly widespread use of the internet and social networking (Facebook, Twitter, etc.). Google introduced their electronic mail system called gmail (2004). Many privacy issues emerged especially after the Patriot Act (2001) gave the US government expanded powers of surveillance of anyone who might be suspected of terrorism. The Advanced Encryption Standard (AES) [11] officially replaced the Data Encryption Standard (DES) [8] in 2001. The US government began accelerating efforts to secure cyberspace and critical infrastructure while developing countermeasures against cyberterrorism and the threat of cyberwarfare [12, 13]. A continuing series of government, military and corporate data breaches made news headlines on a regular basis. Many individuals became victims of various forms of internet fraud including phishing attacks designed to get their passwords or other personal information through electronic mail.

The decade of 2010 continued to see major corporate and government security breaches. The Office of Personnel Management (OPM) had social security numbers and data of millions of persons (e.g., social security numbers) stolen. The decade also brought with it the concept of cloud computing and the Internet of Things (IoT) both of which presented new security and privacy challenges. Evidence emerged


Here you have, ;o) - Message (Plain Text)
File Edit View Insert Format Tools Actions Help
Reply
Reply to All
Forward

From: Darth Sidious [Sidious@Sith.Net] Sent: Sat 2/12/00 03:09 PM
To: Sidous
Cc:
Subject: Here you have, ;o)

```
Hi:
Check This!
```

AnnaKournik...
(2KB)

Fig. 1.3 Spread of computer virus by electronic mail

about the widespread hacking of US computer networks by foreign countries [3]. Software for exploiting computer security vulnerabilities such as Metasploit [14] and Kali Linux continued to increase in popularity [14]. A plethora of computer-security-related conferences (such as DefCon) and websites arose which allowed people to share information about and learn about exploiting computer vulnerabilities. Evidence released by whistleblower NSA contractor Edward Snowden indicated that the US government was working with companies such as Microsoft, Google and Apple and Facebook to access personal information about their clients. Information warfare on a large scale seemed to play a more dominant role in deciding the outcome of US presidential elections than ever before.

1.3 Computer Security Vulnerabilities and Threats

The main goals of computer security are to protect the computer from itself, the owner and anything external to the computer system and its owner. This includes mainly forces of nature (earthquakes, hurricanes, etc.) and individuals known as intruders or attackers. Probably the single biggest threat to computer system security are the individuals (i.e., attackers) who employ a variety of mechanisms to obtain data or resources of a computer system without the proper authorization. A standard part of threat modelling for any system is to identify what might motivate an attack on that system and who might be motivated to attack it. This section includes an overview of the major computer security threats being faced today by computer systems and their users. This includes intrusion by various means, physical access, social engineering, password attacks, computer viruses, malware, botnets and denial-of-service attacks.

1.3.1 The Attacker (Intruder)

An intruder is someone who seeks to breach defenses and exploit weaknesses in a computer system or network. Attackers may be motivated by a multitude of reasons such as profit, protest, challenge or recreation. With origins in the 1960s anti-authority counterculture and the microcomputer bulletin board scene of the 1980s many of these attackers are inspired by documented exploits that are found on alt.2600 newsgroup and Internet Relay Chat (IRC). The subculture that has evolved around this type of individual is often referred to as the computer underground. Attackers may use a wide variety of tools and techniques to access computer systems [14, 15]. If the intruder can gain physical access to a computer, then a direct access attack is possible. If that is not the case, then the intruder will likely attack across a network, often hiding behind a proxy server, vpn tunnel or onion router/tor browser [16].

1.3.2 Physical Access

An unauthorized user gaining physical access to a computer is most likely able to directly copy data from it. Even when the system is protected by standard security measures such as the user account and password it is often possible to bypass these mechanisms by booting another operating system or using a tool from a CD-ROM to reset the administrator password to the null string (e.g., Hiren Boot disk). Disk encryption [17] and Trusted Platform Module [18] are designed to prevent these kinds of attacks.

1.3.3 Social Engineering and Phishing

Social engineering involves manipulation of people into performing actions or giving out confidential information [15]. For example, an attacker may call an employee of a company and ask for information pretending to be someone from the IT department. Phishing is the attempt to acquire sensitive information such as usernames, passwords and credit card details directly from users [15]. Phishing is typically carried out by email spoofing and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. As it involves preying on a victim's trust phishing can be classified as a form of social engineering [15].

1.3.4 Attacker Software Tools

To gain access the attacker must either break an authentication scheme or exploit some vulnerability. One of the most commonly used tools by attackers is Nmap [14].

Nmap (Network Mapper) is a security scanner used to discover hosts and services on a computer network thus creating a “map” of the network. Nmap sends specially crafted packets to the target host and then analyses the responses. Nmap can provide a wealth of information on targets including open port numbers, application name and version number, device types and MAC addresses.

Once a target host and open ports are identified the attacker then typically tries using an exploit to gain access through that port. One of the most powerful tools is Metasploit [14] which has already made code to inject to perform the exploit. Metasploit also takes advantage of other operating system vulnerabilities such as stack or buffer overflow and can also perform privilege escalation. Metasploit can also perform SQL injection [1, 14] which is a technique where SQL statements are inserted into an entry field for execution. SQL injection exploits a security vulnerability that takes advantage of incorrectly filtered or misinterpreted user input.

1.3.5 Botnets

The word botnet is a combination of the words robot and network. A botnet is a number of Internet-connected computers under control of an attacker that are typically used to send spam email or participate in distributed denial-of-service attacks [1] (Fig. 1.4). Botnets can contain hundreds of thousands or even millions of computers. Botnets can be rented out to other attackers for a fee that can be untraceable if paid, for example, in bitcoins [19]. Phishing emails or other techniques are used to install program code in the target computer also known as zombies. The attacker takes great care to ensure that the control messages cannot easily be traced back to them.

1.3.6 Denial-of-Service Attack

Denial-of-service (DoS) attacks [1] are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked. Or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule many forms of denial-of-service attacks are possible. When the attack comes from a large number of points such as in the case of a distributed denial-of-service attack (DDOS) and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the

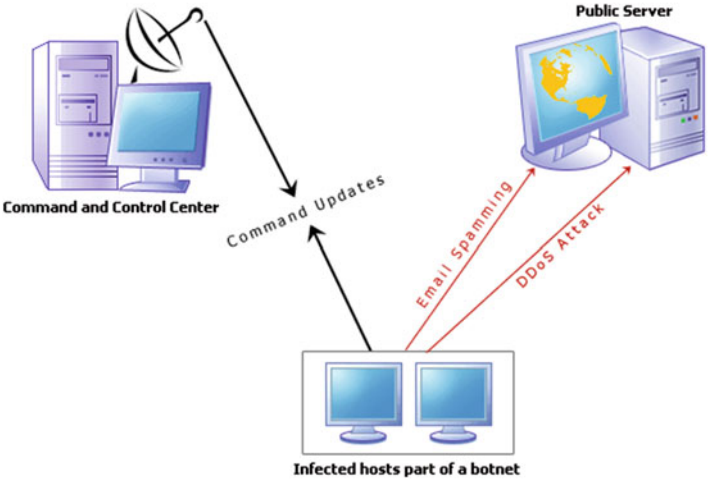


Fig. 1.4 Anatomy of a typical botnet

victim. Denial-of-service attacks are often used in an attempt to cause economic loss to the victim (usually a competitor) and to damage their reputation by making the outage appear to be their fault.

1.3.7 Password Cracking

Perhaps the easiest way to find out a user's password is through social engineering [15]. For example, some people write down their password on a yellow sticky pad and then post it on the wall next to their desk in case they forget it. If direct access or social engineering is not possible, the attacker can attempt to use widely available tools to attempt to guess the passwords. These tools work by dictionary attack of likely passwords and variations of those passwords possibly incorporating user's personal information such as birthdate or the name of their dog. Password cracking tools can also operate by brute force (i.e., trying every possible combination of characters). Lists of possible passwords in many languages are widely available on the Internet. Password cracking tools allow attackers to guess poorly chosen passwords. In particular, attackers can quickly recover passwords that are short, dictionary words, simple variations on dictionary words or that use easy to guess patterns.

Computer systems normally do not store user passwords instead it stores a hash of the password. A hash is a one-way mathematical function. If you know the password, you can easily compute the hash. However, if you only know the hash, you cannot easily compute the password. In some cases it might be possible to copy the entire file of hashed passwords from a system. Normally it is computationally infeasible to reverse the hash function to recover a plaintext password. However, there is a time space trade-off [20] that can be used that might in some cases be able to recover passwords from the hashed password file. Rainbow tables are precomputed hash tables that allow expedited search for a password since the time consuming step of computing the hash has been eliminated. Attackers can spend weeks or months if necessary using rainbow tables to find passwords since the password file has no mechanism for preventing this type of attack.

1.3.8 Malware

One of the most common and well-known threats to computer systems is “malware” which includes computer viruses [21]. A computer virus is a software program that installs itself without the user’s consent then replicates by copying its own source code infecting other computer programs or the operating system itself (e.g., a boot virus). A computer virus often spreads itself by electronic mail (Fig. 1.3.) and attachments to the email that can contain executable code. Malicious software or “malware” includes computer viruses along with many other forms of malicious software such as computer worms, ransomware, trojan horses, keyloggers, rootkits, spyware, adware and other malicious software. Malware often performs some type of harmful activity on infected host computers such as accessing private information, corrupting data, logging keystrokes, creating botnets or providing a backdoor for future access.

The majority of viruses target systems running Microsoft Windows employing a variety of mechanisms to infect new hosts and using anti-detection strategies to evade antivirus software. Motives for creating viruses can include financial gain or simply a sociopathic desire to harm large numbers of people. The Virus Creation Laboratory (VCL) was one of the earliest attempts to provide a virus creation tool so that individuals with little to no programming expertise could create computer viruses. A hacker dubbed “Nowhere Man”, of the NuKE hacker group, released it in July 1992.

1.3.9 Software Piracy

Software piracy is a major computer security issue for organizations that develop proprietary software products. It relates mainly to violation of copyright laws where individuals download software from the internet and make use of that software without compensating the software developer. The cost of software products ranges from free to several hundreds of dollars or more. Peer-to-peer networks are often used to circumvent copyright laws [1] and allow distribution of copyrighted materials and proprietary software to unauthorized individuals. Countermeasures usually involve some type of product code that is needed to activate the software.

Perhaps the most well-known example of this is the product key and activation process that is necessary to install and use many Microsoft operating systems and proprietary software products. Intruders often use reverse engineering techniques such as decompiling the machine language code to circumvent the various software protection mechanisms [22].

1.4 Countermeasures

There are many different ways of gaining unauthorized access into computers and computer systems. It can be done through a network, system, Wi-Fi connection or physical access. Computer systems can be protected by properly designed software and hardware that can help and prevent security failure and loss of data. To secure a computer system it is important to understand the attacks that can be made against it. One of the main techniques used in computer security is the separation of the intruders from the computer or data and this separation can be typically either physical, logical, cryptographic or temporal [1].

In computer security a countermeasure is a technique that reduces a threat, a vulnerability or an attack by eliminating or preventing it or by minimizing the harm it can cause or by discovering and reporting it so that corrective action can be taken. The countermeasures will vary depending on the system to be secured. A risk analysis can also help to determine appropriate countermeasures. Not all security breaches can be detected as they occur so some type of auditing should be included as an integral part of computer security. Audit trails track system activity so that when a security breach occurs the mechanism and extent of the breach can be determined. Storing audit trails remotely can help to prevent intruders from covering their tracks by preventing them from modifying the audit log files.

1.4.1 Authentication

Authentication is the act of verifying a claim of identity and is one of the primary techniques of separation used in computer security [23]. Across the internet you cannot see the person who is trying to access a website. If the person provides the proper credential, they are allowed access. This is one of the areas of computer security of most vulnerability. Passwords are by far the most predominant means of authentication in use today because of the ease of implementation and low cost. Biometric authentication [24] (for example, fingerprints, face recognition, hand geometry, retinal scan, voice recognition) is also in limited use. Strong authentication requires providing more than one type of authentication information (for example, two-factor authentication requires two independent security credentials).

A password is a string of characters used for user authentication to prove identity to gain access to a resource. User names and passwords are commonly used by people during a log in process that controls access to desktop or laptop computers, mobile phones, automated teller machines (ATMs), etc. A typical computer user has many passwords for email, bank account and online e-commerce. Most organizations specify a password policy that sets requirements for the composition and usage of passwords typically dictating minimum length, type of characters (e.g., upper and lower case, numbers, and special characters) and prohibited strings (the person's name, date of birth, address, telephone number). Some passwords are formed from multiple words and may more accurately be called a passphrase. The terms passcode and passkey are sometimes used when the secret information is purely numeric, such as the personal identification number (PIN) commonly used for ATM access.

1.4.2 Data and Operating System Backup

It is not always possible to forsee or prevent security incidents which involve loss of data or damage to data integrity. However, it is possible to be more resilient by having all important data backed up on a regular basis which allows for a faster recovery. Backups are a way of securing information and as such represent one of the main security mechanisms for ensuring the availability of data [1]. Data backups are a duplicate copy of all the important computer files that are kept in another separate location [1]. These files are kept on hard disks, CD-Rs, CD-RWs, tapes and more recently on the cloud. Operating systems should also be backed up so they can be restored to a known working version in case of a virus or malware infection. Suggested locations for backups are a fireproof, waterproof and heat proof safe, or in a separate, offsite location in which the original files are contained. There is another option which involves using one of the file hosting services that backs up files over the Internet for both business and individuals also known as the cloud. Natural disasters such as earthquakes, hurricanes or tornados may strike the building where the computer is located. There needs to be a recent backup at an alternate secure location in case of such kind of disaster. Having recovery site in the same region of the country as the main site leads to vulnerabilities in terms of natural disasters. Backup media should be moved between sites in a secure manner in order to prevent it from being stolen.

1.4.3 Firewalls and Intrusion Detection Systems

Firewalls [2] are an important method for control and security on the Internet and other networks. Firewalls shield access to internal network services, and block certain kinds of attacks through packet filtering. Firewalls can be either hardware or software-based. A firewall serves as a gatekeeper functionality that protects intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks.

Intrusion detection systems [2] are designed to detect network attacks in-progress and assist in post-attack forensics. Intrusion detection systems can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example, trying a lot of passwords to gain access to the network. Honey pots are computers that are intentionally left vulnerable to attackers. They can be used to find out if an intruder is accessing a system and possibly even the techniques being used to do so.

1.4.4 Antivirus and Protection Against Malware

Computer viruses are reputed to be responsible for billions of dollars worth of economic damage each year due to system failures, wasted computer resources, corrupting data and increasing maintenance costs. It is estimated that perhaps 30 million computer viruses are released each year and this appears to be on an increasing trend. Many times a clean installation is necessary to remove all traces of a computer virus as the virus makes many changes throughout the system, for example, the registry in the case of Microsoft Windows systems. In response to the widespread existence and persistent threat of computer viruses an industry of antivirus [25] software has arisen selling or freely distributing virus protection to users of various operating systems. Antivirus scanners search for virus signatures or use algorithmic detection methods to identify known viruses. When a virus is found it removes or quarantines it. No existing antivirus software is able to identify and discover all computer viruses on a computer system.

1.4.5 General Purpose Operating System Security

Most general purpose operating system security is based on the principle of separation by controlling who has access to what and this information is kept in an access control list (ACL). The ACL is modifiable to some extent according to the rules of mandatory access control and discretionary access control [1]. The ACL itself must be secure and tamperproof otherwise an attacker can change the ACL and get whatever access they want.

1.4.5.1 NTFS Security

New Technology File System (NTFS) is a proprietary file system developed by Microsoft. It has replaced FAT and DOS in the late 1990s and has been the default filing system for all Microsoft Windows systems since then. NTFS has a number of improvements over the File Allocation Table (FAT) filing system it superceded such as improved support for metadata and advanced data structures to improve performance, reliability and disk space use. Additional improvements include security based on access control lists (ACLs) and file system journaling. In NTFS, each file or folder is assigned a security descriptor that defines its owner and contains two access control lists (ACLs). The first ACL, called discretionary access control list (DACL), defines exactly what type of interactions (e.g., reading, writing, executing or deleting) are allowed or forbidden by which user or groups of users. The second ACL, called system access control list (SACL), defines which interactions with the file or folder are to be audited and whether they should be logged when the activity is successful or failed.

1.4.5.2 MAC OSX and Linux Security

MAC OSX and Linux have their roots in the UNIX operating system and derive most of their security features from UNIX. A core security feature in these systems is the permissions system. All files in a typical Unix-style file system have permissions set enabling different access to a file which includes “read”, “write” and “execute” (rwx). Permissions on a file are commonly set using the “chmod” command and seen through the “ls” (list) command. Unix permissions permit different users access to a file. Different user groups have different permissions on a file. More advanced Unix file systems include the access control list concept which allows permissions to be granted to additional individual users or groups.

1.4.5.3 Security Enhanced Linux (SE Linux)

NSA security-enhanced Linux [26] is a set of patches to the Linux kernel and some utilities to incorporate a mandatory access control (MAC) architecture into the major subsystems of the kernel. It provides an enhanced mechanism to enforce the separation of information based on confidentiality and integrity requirements which allows threats of tampering and bypassing of application security mechanisms to be addressed and enables the confinement of damage that can be caused by malicious or flawed applications. A Linux kernel integrating SE Linux enforces mandatory access control policies that confine user programs and system server access to files and network resources. Limiting privilege to the minimum required reduces or eliminates the ability of these programs to cause harm if faulty or compromised. This confinement mechanism operates independently of the discretionary access control mechanisms.

1.4.6 Program Security and Secure Coding

Program security reflects measures taken throughout the Software Development Life Cycle (SDLC) [27] to prevent flaws in computer code or operating system vulnerabilities introduced during the design, development or deployment of an application. Programmer reviews of an application's source code can be accomplished manually in a line-by-line code inspection. Given the common size of individual programs it is not always practical to manually execute a data flow analysis needed in order to check all paths of execution to find vulnerability points. Automated analysis tools can trace paths through a compiled code base to find potential vulnerabilities. Reverse engineering techniques [27] can also be used to identify software vulnerabilities that attackers might use and allow software developers to implement countermeasures on a more proactive basis, for example, to thwart software piracy [27].

Securing coding [28] is the practice of developing computer software in a way that guards against the introduction of security vulnerabilities. Defects, bugs and logic flaws are often the cause of commonly exploited software vulnerabilities. Through the analysis of large numbers of reported vulnerabilities security professionals have discovered that most vulnerabilities stem from a relatively small number of common software programming errors. By identifying coding practices that lead to these errors and educating developers on secure alternatives, organizations can take proactive steps to help significantly reduce vulnerabilities in software before deployment.

1.4.7 CyberLaw and Computer Security Incidents

It is very important to bring cybercriminals to justice since the inability to do so will inevitably inspire even more cybercrimes. Responding to attempted security breaches is often very difficult for a variety of reasons. One problem is that digital information can be copied without the owner of the data being aware of the security breach. Identifying attackers is often difficult as they are frequently operating in a different jurisdiction than the systems they attempt to breach. In addition they often operate through proxies and employ other anonymizing techniques which make identification difficult. Intruders are often able to delete logs to cover their tracks. Various law enforcement agencies may be involved including local, state, the Federal Bureau of Investigation (FBI) and international (Interpol). Very rarely is anyone ever arrested or convicted of initiating the spread of a computer virus on the internet [29].

Application of existing laws to the cyberspace has become a major challenge to Law Enforcement Agencies (LEA). Some of the main challenges are the difficulties involved in enforcing cyberlaws and bringing cybercriminals to justice. International legal issues of cyber attacks are complicated in nature. Even if a Law Enforcement Agency locates the cybercriminal behind the perpetration of a cybercrime it does not guarantee they can even be prosecuted. Often the local authorities cannot take action due to lack of laws under which to prosecute. Many of the laws we have today were written hundred of years ago before computers were invented and information in digital form did not exist. Identification of perpetrators of cyber crimes and cyber attacks is a major problem for law enforcement agencies.

1.5 Summary and Future Trends

The future of computer security appears to be that of a never-ending arms race between the attackers and the computer system users and administrators, designers and developers of hardware, software and operating systems. The average computer system user does not have extensive security training but nonetheless has to face the reality of computer security threats on a daily basis. For example, most people have to deal with a large number of passwords for different devices and websites. For that reason it can be expected that we will see a trend toward greater usability in security, for example, a trend toward password manager software [30] or perhaps the elimination of passwords altogether (https://techcrunch.com/2016/05/23/google-plans-to-bring-password-free-logins-to-android-apps-by-year-end/). One way that this could be done is to use the built-in signature of individual behaviours to act as an inexpensive biometric authentication (https://techcrunch.com/2016/05/23/google-plans-to-bring-password-free-logins-to-android-apps-by-year-end/) or by putting authentication into a computer chip [23].

The average person is relatively unsophisticated and is likely to be unaware of computer system vulnerabilities and even if they were they probably would not know how to deal with them. Therefore we can expect to see a trend toward building security into computing systems especially moving it from software into hardware where it is more difficult to compromise. The Next Generation Secure Computing Base initiative and the Trusted Platform Module [18] represent a step in that direction, however, it is not clear how long it will take before that type of technology reaches the consumer market. Secure coding practices [28] are likely to lead to incremental improvements in program and web application security as time goes on.

An overall sense of complacency seems to prevail currently for both computer users and manufacturers. The goal of a secure cyberspace seems to be replaced with a lesser goal of not allowing the situation to get any worse and simply trying to manage the security issues as best as possible as they arise. The current state of security complacency also appears to have become somewhat institutionalized. The number of computer viruses increases each year but no one is ever arrested or convicted as a result [29]. Manufacturers have little motivation to improve security as customers are more focused on features. Critical infrastructure is being increasingly controlled via computer programs that expose new vulnerabilities. Vulnerabilities will continue to be discovered and operating systems will continue to be patched, however, the operating systems in use now have not significantly improved from a security perspective since they were developed in the 1970s and 1980s. Improvements in computer security are not likely to occur proactively rather reactively as a result of cyberwarfare or cyberterroristic events [12, 13].

References

1. Pfleeger, C. P., & Pfleeger, S. L. (2015). *Security in computing* (5th ed.). Upper Saddle River, NJ: Prentice Hall. ISBN:978-0134085043.
2. Stallings, W. (2016). *Cryptography and network security: Principles and practice* (7th ed.). London: Pearson. ISBN:978-013444284.
3. Clarke, R. A. (2011). *Cyber war: The next threat to national security and what to do about it*. Manhattan, NY: Ecco Publishing. ISBN 978-0061962240.
4. Boyer, S. A. (2010). *SCADA supervisory control and data acquisition* (p. 179). Research Triangle Park, NC: ISA-International Society of Automation. ISBN:978-1-936007-09-7.
5. Cohen, F. (1987). Computer viruses. *Computers & Security, 6*(1), 22–35. doi:10.1016/0167-4048(87)90122-2.
6. Caddy, T., & Bleumer, G. (2005). Security evaluation criteria. In H. C. A. van Tilborg (Ed.), *Encyclopedia of cryptography and security* (p. 552). New York: Springer.
7. Stoll, C. (1988). Stalking the wily hacker. *Communications of the ACM, 31*(5), 484–497.
8. *FIPS 46-3: Data encryption standard*. csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf
9. Loukides, M., & Gilmore, J. (1998). *Cracking DES: Secrets of encryption research, wiretap politics, and chip design* (pp. 800–822). San Francisco, CA: Electronic Frontier Foundation.
10. Benton, K. (2010). *The evolution of 802.11 wireless security*. Las Vegas, NV: University of Nevada.
11. Daemen, J., & Rijmen, V. (2002). *The design of Rijndael: AES – the advanced encryption standard*. Berlin: Springer. ISBN 3-540-42580-2.
12. Singer, P. W., & Friedman, A. (2014). *Cybersecurity: What everyone needs to know*. Oxford, UK: Oxford University Press. ISBN:978-0199918199.
13. Clarke, R. A. (2011). *Cyber war: The next threat to national security and what to do about it*. Manhattan, NY: Ecco Publishing. ISBN 978-0061962240.
14. Kennedy, D. (2011). *Metasploit: The penetration tester's guide*. San Francisco, CA: No Starch Press. ISBN:978-1-59327-288-3.
15. Conheady, S. (2014). *Social engineering in IT security: Tools, tactics and techniques*. New York City, NY: McGraw-Hill. ISBN:978-00071818464. (ISO/IEC 15408).
16. Smith, J. (2016). *Tor and the dark net: Remain anonymous and evade NSA spying*., ISBN:978-00071818464978-0692674444. New Delhi: Pinnacle Publishers.
17. Fruhwirth, C. (2005). *New methods in hard disk encryption. Institute for computer languages: Theory and logic group (PDF)*. Vienna: Vienna University of Technology. ISBN: 978-00071818464978-0596002428.
18. England, P., Lampson, B., Manferdelli, J., Peinado, M., & Willman, B. (2003). A trusted open platform (PDF). *Computer, 36*(7), 55–62.
19. Nakamoto, S. (2009). *Bitcoin: A peer-to-peer electronic cash system* (PDF). Retrieved February 20, 2017, from https://bitcoin.org/bitcoin.pdf
20. Hellman, M. E. (1980). A cryptanalytic time-memory trade-off. *IEEE Transactions on Information Theory, 26*(4), 401–406. doi:10.1109/TIT.1980.1056220
21. Aycock, J. (2006). *Computer viruses and malware* (p. 14). New York: Springer. ISBN: 978-00071818464.
22. Eilam, E. (2005). *Reversing: Secrets of reverse engineering*. Indianapolis, IN: Wiley Publishing. ISBN:978-0007181846413-978-0-7645-7481-8.

23. Richard E. S. (2001), Authentication: From passwords to public keys., ISBN: 978-00071818464978-0201615999.
24. Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*(2), 91–98. doi:10.1145/328236.328110
25. Szor, P. (2005). *The art of computer virus research and defense*. Boston: Addison-Wesley Professional. ASIN 0321304543.
26. *National Security Agency shares security enhancements to linux*. NSA Press Release. Fort George G. Meade, Maryland: National Security Agency Central Security Service. 2001-01-02.
27. Sommerville, I. (2015), Software engineering., ISBN:978-0133943030.
28. Graff, M. G., & van Wyk, K. R. (2003). *Secure coding: Principles and practices*. Sebastopol, CA: O'Reilly Media, Inc.
29. *List of computer criminals*. https://en.wikipedia.org/wiki/List_of_computer_criminals
30. Li, Z., He, W., Akhawe, D., & Song, D. (2014). *The emperor's new password manager: Security analysis of web-based password managers (PDF)*. Usenix.