CHAPTER 2

History of Computer Security

Introduction

The first events in the history of exploiting security date back to the days of telephony. Telephone signals were sent via copper cables. Telephone lines could be tapped and conversations could be heard. In the early days of telephone systems, telephone operators intentionally misdirected calls and eavesdropped on conversations. In the 1970s, a set of people known as phreakers exploited the weakness of digital switching telephone systems for fun. Phreakers discovered the signal frequency at which the numbers are dialed and tried to match the frequency by blowing a whistle and fooling the electronic switching system to make calls for free. Among these phreakers, John Draper found that he could make long-distance calls for free by building an electronic box that could whistle different frequencies.

During the 1960s and 1970s, telephone networks became the dominant mode of communication, connecting millions of users. Given the increasing importance of computers and the advent of time shared systems, it was natural to consider linking the computers on the telephone networks so that information could be shared among geographically distributed networks. Since telephones were analog and computers were digital, modem (modulator and demodulator) devices were used to connect computers over the telephone network. Connecting computers and sharing information was of major interest during the early days of network computing and the security of the information became weak. Since people already knew how to break and tap into the phone systems, it became a game for them to break into the computer system, which was connected over the telephone networks.

With the creation of Advanced Research Projects Agency Network (ARPANET), a limited form of a system break-in to the network began. ARPANET was originally designed to allow scientists to share data and access remote systems. E-mail applications became the most popular application to allow scientists to collaborate on research projects and discuss various topics over the network. Soon, a bulletin message board was created where people could post a topic and discuss various research topics together. Bulletin boards became the venue of choice for discussing a wide range of topics, including passwords, credit card numbers, and trade tips, which encouraged the bad guys to hack into the system. Some famous bulletin boards include Sherwood Forest and Catch-22.

WHAT IS ARPANET?

The predecessor of the Internet, the Advanced Research Projects Agency Network (ARPANET) was a large wide-area network created by the United States Defense Advanced Research Project Agency (ARPA). Established in 1969, ARPANET served as a testing ground for new networking technologies, linking many universities and research centers. The first two nodes that formed the ARPANET were UCLA and the Stanford Research Institute, followed shortly thereafter by the University of Utah. Some of the reasons for creating ARPANET include making it easier for people to access computers, to improve computer equipment, and to have a more effective communication method for the military.

In the 1980s, the TCP/IP network protocol Transmission Control Protocol (TCP) and the Internet Protocol (IP), and Personal Computers (PC) brought computing to homes where more and more people connected to the Internet. The 1983 fictional movie, "War Games," was watched by millions of people and popularized hacking and made it glamorous. In 1981, Ian Murphy broke into AT&T's computers and changed billing rates of meters. He was later convicted.[1] Kevin Mitnick stole computer manuals of Pacific Bells' switching center in Los Angeles, California, and was prosecuted for this crime.[1] Bill Landreth was convicted for breaking into NASA's Department of Defense computers through GTE's e-mail network. In 1988, Kevin Mitnick was held for stealing software that was worth $1 million, and also caused damages of around $4 million.

With increasing threats to security, government agencies in charge of ARPANET came up with the Computer Emergency Response Team (CERT): the first network security organization in 1988.[2] The purpose of CERT is to spread security awareness among users and find ways to mitigate security breaches. As the Internet became popular, with more and more users becoming active, it became an appealing target for the "hackers" around the world. The 1990s saw more hacking activities such as the "Michelangelo" virus and the arrest of notorious hacker Kevin Mitnick for stealing credit card data, and the 1998 Solar Sunrise attack targeting Pentagon computers by Ehud Tenebaum.[3]

Today we are living in the Internet and World Wide Web (WWW) era, where everyone is connected. The Internet has changed the way we communicate with each other. The Web allowed information to be accessed instantly from anywhere in the world. First-generation web 1.0 was just a static web. Web 2.0, called interactive web, allowed the users to communicate by emphasizing online collaboration. Web 3.0 technology called 'the intelligent Web' emphasized machine-facilitated understanding of information to provide a more intuitive user experience. The Web has become a social medium where we can interact with one another, which has unfortunately resulted in many threats and vulnerabilities and an increasing number of security breaches. Some of the popular attacks include "Mellisa, the love bug," the "killer resume," and "The code red."

Communication

Communication is about conveying messages to the other party or to a group. These messages carry certain information. The medium through which information is communicated can be words or signs. The basic need to communicate has evolved languages, and language is used as a medium to share information, ideas, and feelings. There are three main types of communication: oral communication, written or verbal communication, and non-verbal communication.

During oral communication, parties communicate through voice as a medium. The parties involved in the oral communication are expected to be able to convey the message, which clearly expresses all their feelings, needs, wants, values, beliefs, and thoughts. Again, both the sender and the receiver use the same language so that both can understand. The sender can speak and the receiver can listen and vice versa, in order to exchange information. The tone of voice or the gap of silence makes a huge difference in oral communication.

During non-verbal communication, the communication is through the use of body language, gestures, facial expressions, and signs. These expressions may be well structured or unstructured. The semaphores that were used by military, sign language used by deaf persons, and gestures, postures, facial expression, and eye contact used by humans are a few of the examples. Semaphore Flags are the telegraphy system that conveys information at a distance by means of visual signals with handheld flags, rods, disks, paddles, or occasionally bare or gloved hands. Information is encoded by the position of the flags and is read when the flag is in a fixed position. Semaphores were adopted and widely used (with hand-held flags replacing the mechanical arms of shutter semaphores) in the maritime world in the nineteenth century. It is still used during underway replenishment at sea and is acceptable for emergency communication in the daylight or while using lighted wands instead of flags at night. Even verbal communication may have underlying non-verbal signals like stress, rhythm, and intonation, which may convey a different meaning to the person tuned to such signals or intended recipients of such signals. Non-verbal communications can be considered coded and may have different meanings to different recipients. Many times, non-verbal communication or gestures complement or negate the words spoken and may emphasize the words spoken or give them a different meaning than the meaning of the words spoken. Strong observation and hearing is required to understand the non-verbal communications, particularly if they are embedded with secret signals.

Sometimes, information needs to be communicated to only a few people and understood by only a few people, like the messages sent by kings, military commanders, diplomats, and other military people. Since the early days of writing, kings and commanders in India used secret codes to send messages to other kings and commanders outside the state. During war time, secret messages were sent by a network using simple alphabetic substitutions often based on phonetics. The ancient Chinese used the ideographic nature of their language to hide meanings of words. In the past, sensitive messages were transported through trusted persons, were guarded and were stored in a secure environment, thus ensuring the security of information. Julius Caesar (50 B.C.) is credited with the invention of cipher code to protect the confidentiality of information in order to prevent secret messages from being read by others. The Caesar cipher is named after Julius Caesar, who used simple coding techniques to protect messages of military significance. Caesar used a simple technique of replacing each letter in the plaintext by a letter shift of 3. He used this method for all his military communications.[4]

It is unknown how effective the Caesar cipher was at that time, but there are incidences in the nineteenth century where the personal advertisements section in newspapers would sometimes be used to exchange messages encrypted using simple cipher schemes. According to Kahn (1967), there were instances of lovers engaging in secret communications coded in Caesar cipher in *The Times* personal ads. More complicated Caesar cipher was also in use by the Russian army during war times because it was difficult for their enemies to decipher.[5]

The need for communication not only helped in the development of many languages, but also the basic need to communicate with those at a distance resulted in the invention of telegraphs and telephones. The telegraph is a communication system invented by Samuel Morse (1791–1872), in which information is transmitted over a wire through a series of electrical pulses called Morse code. Morse code is a series of dots and dashes.[6] The pattern of dots and dashes were assigned to letters of the alphabet, numerals, and punctuation marks. Telegraph operators used Morse code to code the plain text messages before transmission over the electric cable and at the receiving end, where operators translated the Morse code back to plain English. The electric telegraphs transformed how wars were fought, and how military commanders sent their messages to distant soldiers and commanders. Rather than taking weeks to deliver messages by horse carriages and trusted messengers, information could be exchanged between two telegraph stations almost instantly. There are records of using telegraph systems during the Crimean war of 1853–1856. In the 1860s, the Russian army used telegraphs for communication between field officers and headquarters. After the telegraph, further inventions led to distance-based communication, such as radio and telephone.

During the early days of distance-based communications, messages were disguised to protect the confidentiality and to avoid them being revealed to others. It is natural that the messages sent through the telegraph, telephone, and eventually the radio, were also expected to be disguised in the form of codes. With the advent of distance communication methods using radio signals, the use of cryptography became very important, especially for coordinating military operations. Historically, we know that the French, American, and German armies were actively using various kinds of cipher methods during World War I.

World Wars and Their Influence on the Field of Security

There is no doubt that the world wars had significant influence on the field of security. As the adage goes, "Necessity is the mother of invention." In the interest that secrets are preserved and conveyed safely, new ways of securing the information were explored, invented, and practiced. These efforts have provided many solutions to today's problems and had set things in the right direction for further invention and innovation. Many of today's security practices originated somewhere during the world wars.

Cypher Machine: Enigma

Telegraphs, telephones, and radios have changed the meaning of communication. The demand for these services came from the railroads, the press, business and financial sectors, and private citizens. However, it became even more important for military communication. The telegraph led to considerable improvements in the commanding of troops, but it also required qualified specialists. The invention of the telephone by Alexander Graham Bell in 1876 opened a new sphere of communication. Telephone connections required a significant amount of cabling, power,

and time for laying, and the same cable could not be used for both a telephone and telegraph. The invention of the radio became one of the greatest inventions in world history. Guglielmo Marconi was an Italian inventor who invented radio communication in 1895 which changed the world of communication, particularly in the military. However, messages sent through these devices were not protected and could be overheard by others. Messages sent over a telegraph line or radio link cannot be packed in an envelope and anyone who has access to the lines or a radio receiver could intercept messages and read everything without being identified. Thus emerged the need for secure communication for the military as well as civilians and has become essential that even when messages are heard, nobody other than the intended listeners should make out the contents.

Most pre-World War II military communication relied on the simple shuffling of words or a number representation for each word. Other methods were easily decipherable using frequency analysis. During this time, Enigma emerged as a means of communication due to its complex encryption methods.

In 1919, Dutchman Hugo Alexander Koch constructed one of the world's first electromechanical rotor machines for encrypting and decrypting messages called the Enigma. Initially, he thought he could sell these machines to banks to make secure transactions over regular telephone and telegraph channels. But neither banks nor the government showed any interest. After a few years, the patent went to Arthus Scheribus, who sold these machines to the German government.[7]

The strength of the Enigma, shown in Figure 2-1, gave Germans complete confidence in the security of their messages during military operations. In fact, Germans changed the coding keys every three months until 1935, and then monthly until 1936. During the war in 1943, keys were changed every eight hours. The "invincible" German secret machine was one of the most important milestones of World War II. Without breaking Enigma, World War II would have taken a different course and would have been extended for a few more years.[7,8]

Figure 2-1. *The German Wehrmacht Enigma (Copyright © 2014 Dirk Rijmenants)*[9]

During war time, Germans used Enigma to encode military commands over the radio. Enigma is an electromechanical device where you can set the rotor to a certain position and type the message just like a typewriter, for a mechanically encoded message. The intended receiver needed to know the exact position of the rotor in order to decode the message. The basic three-rotor Enigma with a 26 X 26 X 26 had 17,576 possible combinations of rotor states. The Enigma had three normal rotors and one reflector that could be set in one of 26 positions. For ten pairs of letters connected to each rotor and six wheels, there could be as many as 150,738,274,937,250 possible states. This gave the Germans a huge advantage in the war. Each time the messages were generated using a different set of combinations and with billions of combinations, the German military thought that the Enigma messages would remain unbreakable.[7]

Bletchley Park

After Hitler was appointed Chancellor of Germany on January 30, 1933, the Nazi Party began to consolidate their power by conquering neighboring countries. Hitler invaded Poland in September 1939 and thus launched World War II in Europe. Germany conquered most of Europe by 1940, and then threatened Britain next. Britain and her allies were unable to understand the military strategy of Hitler and worried about the use of Enigma and the problem posed by this machine. Breaking the Enigma continued to be a major challenge during World War II. Even the early mainframe computers were put to use to try and break the Enigma code.

The Germans thought that the Enigma code was impossible to break because of the many key combinations. However, Poland's Biuro Szyfrow, based on the Enigma codebook sold by the German spy Hans-Thilo Schmidt, attempted to break the Enigma messages. Three Polish mathematicians – Marian Rejewski, Henryk Zygalski, and Jerzy Rozicki – were convinced that they could break the Enigma. They also developed an electro-mechanical machine, called the Bomba, to break the Enigma code. During this process, they found two major flaws in the design. When Germans invaded Poland, the Polish Biuro Szyfrow passed on all the details and Bombe machines to the troubled French and British intelligence.

Alan Turing, widely known as the father of computer science and artificial intelligence, joined the British Government Code and Cypher School (GC &CS) and set up a secret code-breaking group called "Ultra" at Bletchley Park to break the Enigma code.[10]

Figure 2-2. *Alan Turing (photograph by Colin Smith)*[11]

Turing designed "Bombe" machines that were used to decipher Enigma. The Turing Bombe searched for the enigma settings for a given piece of plain and cipher text. Turing used his mathematical skills to decipher the Enigma codes. Initially, Turing and his colleagues relied on guessing the content based on external information. This helped them to reduce the strength of the key and finally they were able to break the Enigma codes. The Turing machine is one of the major inventions during the world war apart from atom bombs. It is estimated that this work by GC & CS shortened World War II by two years and Turing received the Appreciation Order of the British for the crucial role he played.

Code Breakers

The development of security has a military origin. Since the early days of World War II, breaking into any information is considered another technological challenge. As we described in earlier paragraphs, the German military relied on Enigma to encrypt all military communications in World War II, and to win the war, it became absolutely necessary for the allies to break the Enigma coded communication. The allies finally broke into it under the leadership of Alan M. Turing in Bletchley Park, who expanded further on the work done by the Polish mathematician and cracked the Enigma coded messages using a new machine designed by them known as "Bombe". After winning the war, Winston Churchill reportedly said to George VI: "Thanks to Ultra that we won the war".[12] It was also believed that the war was shortened by two years because they were able to break the Germans' military codes and spoil their strategies. The work done by Turing and his colleagues in Bletchley Park brought a new dimension to cryptography in the modern world. Cryptography required an understanding of logic, statistical theory, information theory, and advanced technology.

In the early days of computers, security was concerned only with the physical device and access to it. Early mainframe computers were used to store government records, personal information, and transactional processing. The security was to safeguard the data stored in the computers. Hence, physical access to the location was guarded and very few personnel had access to this location. Access was only achieved by authorized photo identification. The entry and exit to the computer rooms were monitored to ensure that the device, as well as the data stored in the device, was secured.

The security concerns increased as the technology advanced from single user mainframes to multiuser systems. The UNIX operating system evolved from MULTICS systems, which were originally designed for multi-user access.[13] UNIX is a multi-user, multi-tasking operating system, which allowed multiple users to access the system remotely (multi-user), and each user can run multiple applications simultaneously (multi-tasking). UNIX brought in the concept of authentication for secure access of files and data in a shared environment. The UNIX system was designed to provide the security for accessing files with user IDs and group IDs using sophisticated security programs. However, the system needed to be configured properly. Misconfiguration of the system could lead to the exposure of data and files to other unintended users, thus creating security holes. Much of the UNIX system was developed by students as a research project by including many of networking utilities and protocols. Since these programs were not written with proper design and are not formally tested, earlier versions of UNIX were buggy and could be exploited easily.

Mini computers, Personal Computers (PCs), Client Server architecture and Transmission Control (TCP), and Internet Protocol (IP) revolutionized computer communication. Mainframe computers were connected on the telephone network based on a "circuit switching" of protocols. In 1973, the U.S. Department of Defense, as a part of a research initiative, allowed universities and research organizations to connect to their network using the ARPANET protocol, a "packet switching" protocol. The objective of this project was to develop a communication protocol that would allow computers to communicate transparently across different geographies. This research initiative of ARPANET led to the development of a new protocol, based on packet switching, called TCP/IP (transmission Control protocol) and Internet Protocol. While the ARPANET protocol started as connecting just universities, the TCP/IP protocol opened to the public allowed the connection of millions of users and millions of computers resulting in the Internet – the Internetworking of computers. Today, billions of users are connected across the globe on the Internet which continues to grow exponentially.

The basic need of a computer network is to share information on the network. The TCP/IP protocol suite connects the computers; however, many utilities such as file transfer, remote login, remote shell, telnet, and send mail developed on top of the TCP/IP protocol support information sharing on the Internet. A File Transfer Protocol (FTP) allows files to be transferred from one remote computer to another. A Sendmail protocol allows for the sending and receiving of e-mails from one system to another. With the World Wide Web (WWW) and HTTP protocols, the Internet exploded beyond the sharing of information to doing business on the Internet. Today, the WWW has changed the way we live, how we interact with others, share information, how we buy and sell goods and do business. On the WWW, you can share texts, pictures, images, video, and audio files. To support different applications on the web, multiple utilities and protocols have been developed. With the rise in e-commerce, not only the good guys transact on the web, but we also find many bad guys out there attempting to steal information and make a profit. In response, expectations of information security have changed. Security is no longer just about protecting a physical device, it has now expanded to ensure confidentiality, integrity, authenticity, and availability.

Some Historical Figures of Importance: Hackers and Phreakers

While a set of scientists work toward securing the network and the information that flows on the network, there is another set of phreaks who challenge the scientists by breaking into the network and the information by cracking the security codes. Hackers are intruders who are as capable and knowledgeable as the scientists, but instead of securing the system, they break into the system, thus undoing all the hard work that the scientists have put in. However, there is a new category of security professionals known as ethical hackers, who try to help the industry and governments to unearth the security risks. These are the good guys and are known as the “white hats,” whereas the bad guys are typically known as the “black hats.”

The early days of telephone networking witnessed hackers making long-distance calls without actually paying. Hackers used electronic devices to crack into the telephone network to make long-distance calls (Figure 2-3). The telephone network hackers became popularly known as phreakers. During the same time, the term “cracker” originated as a name for people who crack the system’s security, often by cracking the system’s password.

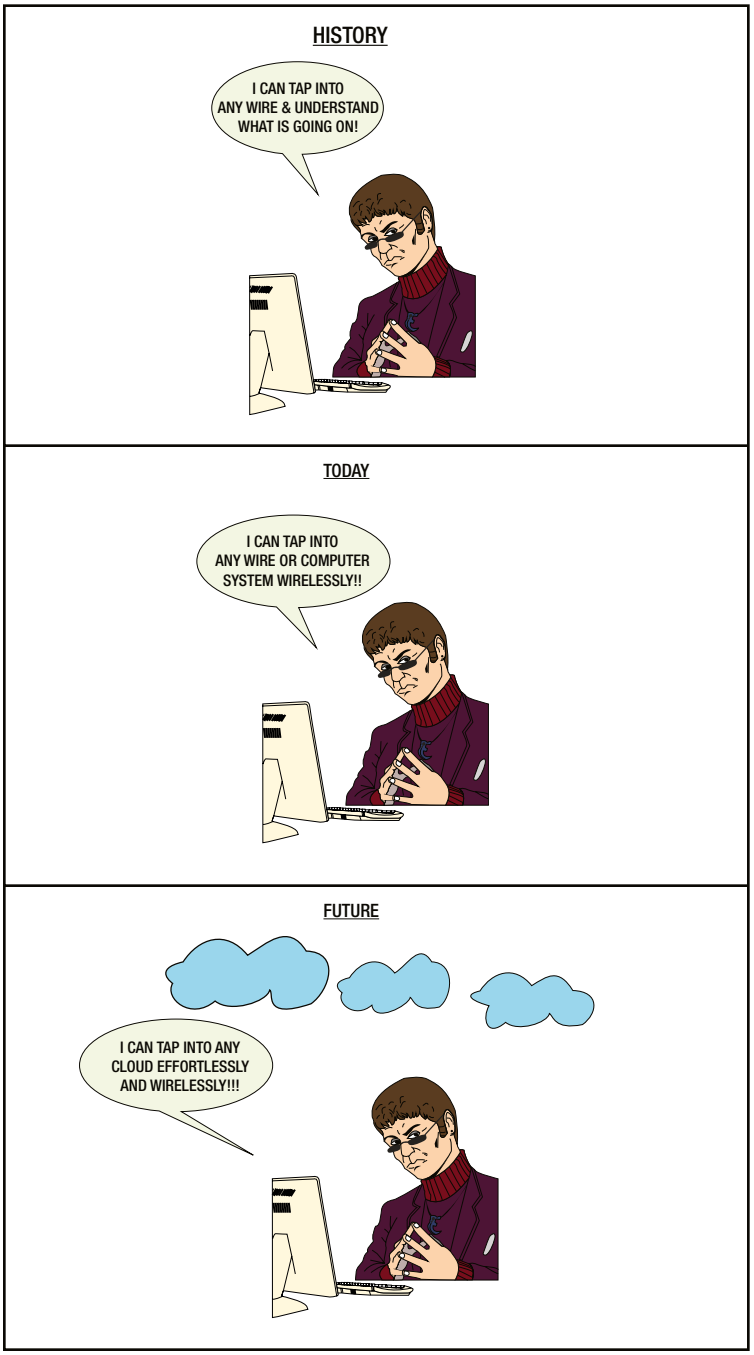

Figure 2-3. *Hackers cracked into telephone networks*

Among the Phreakers, John Draper became famous because of a simple discovery. Earlier telephone systems used in-band signaling for sending control information such as dial tone, busy tone, receiver off-hook, and routing address to the switch in the same channel where the user's voice was being transmitted. Table 2-1 shows the frequency of different control signals. These signals are generated by the Central Office (CO) switch. Subscribers are connected to the CO, and when the phone is off the hook, the CO transmits a 350 and 440 Hertz signal to the subscriber which is the dial tone. A 2600 Hertz frequency tone generates a call over signal and provides control over other signals to make another call again. Similarly, the CO transmits other control signals to the subscriber, which was made public in the Bell Systems Technical Journal.[14,15]

Table 2-1. *Network Call Progress Tone Frequencies*

Tone	Frequency (hz)	On Time	Off Time
Dial	350 + 440	Continuous	
Busy	480 + 620	0.5	0.5
Ringback, Normal	440 + 480	2	4
Ringback, PBX	440 + 480	1	3
Congestion(Toll)	480 + 620	0.2	0.3
Recorder (local)	480 + 620	0.3	0.2
Receiver Off-hook	1400+2060+2450+2600	0.1	0.1

John Draper, shown in Figure 2-4, was discharged from the military because he had knowledge about the telephone systems. After the telephone companies made the control signals public, Draper was anxious to break into the telephone systems. One day, he found out that packaged boxes of Cap'n Crunch cereal could emit a tone precisely at 2600 Hertz. Using Cap'n Crunch boxes, John would blow the whistle to make long-distance calls. This whistle experiment led him to come up with an electronic device called the Blue Box, which would generate different control tones used by the phone company. He succeeded in making long-distance calls from a public telephone without actually ever paying for the calls.[15]

Figure 2-4. *John Draper (Copyright © 2014 The Porticus Centre, Beatrice Technologies)*[16]

Draper popularized this device and became infamous for hacking into telephone systems. He was arrested in May of 1972 for toll fraud charges and was sentenced to a five-year probation. In 1976, he was arrested again for wired fraud charges and spent four months in prison.

Kevin Mitnick

By the 1980s, technology advancement in computers shifted the attention of hackers from phones to computers. With mini-computers, PCs gained popularity and the Internet became a key invention for sharing information. Bulletin Board Systems (BBS) made its appearance where people could post messages on any topic. The BBS became a platform for hackers for their hacking activity. Hackers got into the BBS as normal users and collected users' discussion information, such as credit card numbers, telephone numbers, and e-mail IDs, and pass it on to the hacking community. The BBS was also used by hackers to discuss how to use stolen credit cards, guess computer passwords, and share other users' passwords. In 1986, the government realized the threats to information security and passed the Computer Fraud and Abuse Act, making computer-related abuse a crime across the United States of America.

During the days of ARPANET (before the Internet), users shared jokes and annoying messages with each other, which was not considered a major security issue. Also, the network was small and users knew and trusted each other. Even connecting to the remote system was not considered a major security risk until 1986 when Cliff Stoll published his experience in a book, called *The Cuckoo's Egg*, which described how he connected to a remote computer and copied data from the remote machine without having authorized access. This was the first ever security incident that was formally reported upon. In 1988, Robert T. Morris wrote a computer program that could connect to a remote machine and copy data to another computer and repeat this action over the network. This self-replicating tool, now popularly known as the Morris Worm, exploded on the ARPANET. The worm used up the CPU and system resources of the victim's computer, which after the hack, could not function properly. As a result of this widespread worm, nearly 10% of the computers on the network stopped functioning at the same time. The damage of this worm initiated the Defense Advanced Research Project Agency (DARPA) to form a team to handle computer emergencies called CERT (Computer Emergency Response Team) in 1988. Morris was reprimanded by the U.S. government, was fined $10,000 for damages, put on probation, and was sentenced to community services.

In the 1990s, the Internet gained momentum. The Department of Defense and DARPA made the ARPANET public. A version of the ARPANET protocol, called the TCP/IP, has evolved and the ARPANET became the Internet, connecting thousands of users. After the Internet became public, millions of users and many organizations, universities, and commercial entities became connected to the Internet as well. As the number of Internet users grew, it became difficult for users to trust the network. Resources shared data on the network with other users, thus causing the Internet to become vulnerable to attacks.

Kevin Mitnick, wrote his first hacking program when he was in high school. When a teacher asked the class to write a program to print the Fibonacci number, Kevin wrote a program that could get the passwords of students. His teacher gave him an A for writing this program. His passion for writing programs to crack computers continued. He cracked the computer systems of many companies, such as Digital Equipment Corporation, Motorola, and SUN; all mostly for fun. However, when companies found out that he hacked into their computer systems without authorization, he became a wanted man by the U.S. government. In 1988, he was convicted of copying software from a Digital Equipment Corporation (DEC) and was sentenced with twelve months imprisonment and three years of supervised parole. While he was on parole, he hacked into several computer systems, including Pacific Bell system's voicemail server - the largest telephone network - and stole computer passwords and broke into e-mail servers. After a warrant was issued to arrest him, he fled and became a fugitive for 2 ½ years. Finally, he was arrested in 1995. In 1999, Mitnick confessed to computer fraud and illegally intercepting the communication network and was sentenced to almost four years in prison.[17]

Though Mitnick claimed he did not hack the computer systems for monetary gain, it was still considered illegal according to the U.S. government. Despite his run-ins with the law, Mitnick has influenced modern-day hackers, including WikiLeaks. Today, he spends his time advising companies about the security vulnerabilities in their networks.

Today, the Internet and World Wide Web (WWW) has changed the way we live. According to the latest statistics, more than 3 billion users are on the Internet. Web technologies (Web 2.0) provide many applications and tools that have enabled how we interact on the Internet. Originally just a means of e-mail communication, the Internet is now used for buying, selling, marketing, advertising, channel for B2B, B2C, and many more. This also means the Internet now has different kinds of users connected: trusted or untrusted, good intentioned or bad intentioned. That means the Internet has become more vulnerable to attacks. More and more security incidences are reported at CERT every day. Thousands of intruders are on the Internet and they can:

- Probe: Monitor the network and its users by using tools and tapping the wires.
- Scan: Scan the network and its devices for vulnerabilities, using probing and similar tools.
- Write malicious code: A program or an application that contains harmful code. By installing such an application, your system can be compromised and without your knowledge, it can send your personal data to the remote user. Programs like viruses, worms, and Trojan horses, are a few examples of malicious code.
- Denial of Service: All your system resources could be exhausted or stopped temporarily.
- Gain Access: Gaining unauthorized access to a network, system, and their resources.

In the early days of the Internet, the user groups were relatively small. Intruders exploited relatively simple weaknesses, such as passwords or default configurations of the system. The technique was relatively simple and it worked. During those times, organizations did not have the expertise in configuring systems or tools to monitor the security of the network. Awareness of the scope of the problem was also limited. Today, the importance of security and its awareness has increased among people and networks have become more secure. Consequently, the intruders also have become smarter. Many sophisticated tools have been developed by them and made available to the public. This has become a day-to-day challenge between the good guys and the bad guys.

Today, the most controversial topic related to security is WikiLeaks. WikiLeaks, founded by Julian Assange, is a non-profit organization that is reporting important and confidential news and information to the public on digital media. WikiLeaks provides the evidence, along with the news. The news piece is generally political and is of significant value to society. WikiLeaks has published a number of confidential and classified information. Some of the famous WikiLeaks stories are listed below:

- E-mail contents of Sarah Palin's account (U.S Republican Vice Presidential candidate) in 2008
- Contributors to the Norm Coleman Senatorial campaign (March 2009)
- Communications related to the tax avoidance by Barclays Bank (March 2009)
- Nuclear accident in Iran (2009)
- U.S. Department of Defense Counter-intelligence Report (March 15, 2010)
- "The Global Intelligence Files", containing more than 5 million e-mails from Stratfor, dating from July 2004 to December 2011
- Bradley Manning exposed the truth about America's wars in the Middle East and how the United States conducts foreign policy

WikiLeaks allows any user to upload information anonymously. Users can electronically submit the information without revealing their identity. WikiLeaks uses highly sophisticated technology by providing electronic drop boxes fortified by cutting-edge cryptographic information technology. The site also provides maximum security to the information and their sources.

Bradley Manning, a military personnel, leaked documents to WikiLeaks related to America's wars in the Middle East in 2010 which sparked a global debate about U.S. foreign policy. While Manning was deployed in Iraq, he accessed secure intelligence networks to gather secret military and diplomatic files which he downloaded and

passed on to WikiLeaks. This information was published by WikiLeaks and read by millions of people across the world. Manning was caught when he openly admitted the leaks. According to the U.S. government, he is a traitor who revealed military secrets and put the lives of his comrades-in-arms in danger. Prosecutors argued throughout the trial that the published secret information had directly benefited Al-Qaeda. Manning is facing a 35-year jail term for leaking over 750,000 military and security documents to WikiLeaks.[18]

In June 2013, Edward Snowden a former member of the U.S. National Security Agency, exposed documents and information about both the Internet and phone surveillance by U.S. intelligence on WikiLeaks.[19,20] The documents contained vast information about the domestic surveillance of millions of American citizens under the U.S. government program called PRISM. Though his argument is that the "U.S. government destroys privacy, Internet freedom, and basic liberties for people around the world with this massive surveillance machine they're secretly building," the U.S. government has charged Mr. Snowden with theft of government property, unauthorized communication of national defense information, and willful communication of classified intelligence. Each of the charges carries a maximum of 10 years in prison. Snowden is currently in Russia on temporary asylum.

According to the WikiLeaks web site, WikiLeaks claims that it is working for transparency based on Article 19 of the Universal Declaration of Human Rights. The WikiLeaks web site further defines "principle leaking" as necessary to fight corruption, to uphold individual rights and good governance. In recent days, WikiLeaks has come under severe attack by many governments, particularly the United States, for publishing confidential information on its web site. WikiLeaks has been questioned on the impact of such leaks.

The most high-profile documents published by WikiLeaks are either U.S. government related documents or U.S. government actions against other countries, such as hidden war crimes, prisoner abuse, or individual privacy. After the leak of the content of U.S diplomatic cables and PRISM, the U.S. reaction has been more harsh and the White House Attorney General Eric Holder asserts that WikiLeaks is an increasing threat to national security, America's economy, and is undermining U.S. national security and needs to be stopped. Stephen Aftergood, the director of the Federation of American Scientists Project on Government Secrecy explains that, "It has invaded personal privacy. It has published libelous material. It has violated intellectual property rights. And above all, it has launched a sweeping attack not simply on corruption, but on secrecy itself. And I think that's both a strategic and a tactical error. It's a strategic error because some secrecy is perfectly legitimate and desirable. It's a tactical error because it has unleashed a furious response from the U.S. government and other governments that I fear is likely to harm the interests of a lot of other people besides WikiLeaks who are concerned with open government. It may become harder to support protection for people who disclose and publish classified information after WikiLeaks."

Chapter Summary

- We explored security issues from the days of telephony and discussed how a class of people known as the "phreakers" tried to exploit the weaknesses in telephone systems. We also discussed how the telephonic lines allowed the computers to be connected with each other and how those who could exploit the telephone lines continued to hack into computers with this knowledge. We also looked at how bulletin boards and the information on these bulletin boards were misused. We made a passing reference to some of the legendary hackers and how the increasing threats to computer security led to the CERT initiative.
- We also explored both verbal communication and non-verbal communication. We looked at how secret communications were being conveyed through a coded language using Caesar cipher from the days of Julius Caesar. We also discussed how, with the advent of telegraphs and radio, the need for coding these messages was necessary to protect the confidentiality of these messages.

- We briefly touched upon how the world wars necessitated the securing of messages being relayed and mentioned that most of the current security practices have had their base on the security practices commenced during the world wars. We further explored how the Enigma cipher machine helped Germans in World War II to encode their military messages securely and how the breaking of the Enigma code led to the shortening of World War II.
- We introduced the code breakers and discussed how a great Polish mathematician by the name of Alan M. Turing broke the Enigma code, thus shortening World War II.
- We discussed two famous categories of computer hackers: the "phreakers" and the "hackers". We introduced one of history's famous phreakers, John Draper, who was an expert at hacking and misusing telephone lines. We also discussed one of the most famous hackers, Kevin Mitnick, who could break into almost any computer, including those of big names like DEC, Motorola, and SUN. Additionally, we discussed WikiLeaks, which is a recent phenomenon in the field of computer security and we explained how WikiLeaks brought to the forefront many political secrets.