Chapter 2
Hackers, Crackers, and Phone Phreaks

Chapter Outline

I. Introduction
II. The Evolution of the Term "Hacker"
- A. There are many different definitions available for the term "hacker."
- B. Today, individuals who claim to be hackers argue that true hackers are interested in furthering computer security and that those who do not conform to this belief system are not hackers in the truest sense of the word.
- C. The origin of the term "hacker" can be traced back to the Massachusetts Institute of Technology (MIT), which was one of the first institutions in the United States to offer computer programming and computer science courses.
    1. The term is believed to have first been used in a computer context by the members of the Artificial Intelligence Lab at MIT.
    2. The members began referring to themselves as hackers because they were able to take computer programs and make them perform actions not originally intended by the designers of the computer software.
- D. The term "hacker" remained a relatively obscure term until crimes committed via computer began gaining more publicity in the media.
    1. The term became associated with individuals who were using their personal computers to gain unauthorized access to other individuals' and businesses' computers.
- E. Cracker is generally used to refer to one who violates software copyright protections and gains inappropriate access to password protected files and services.

III. The Introduction of Hacking to the Public
- A. The linking of computers to share resources has raised the level of potential harm to the point where computer-related attacks can impact national, as well as international, security.
- B. It could be considered ironic that technology that was developed as a means of improving research, education, training, and information sharing has developed into one of the most used criminal tools in history.
- C. High-profile media events would introduce the general public to the potential dangers of computer hacking.
    1. Early 1983—a series of rather serious computer break-ins
        a. Discovered that at least 60 computers belonging to the Memorial Sloan-Kettering Cancer Center and the Los Alamos National Laboratory were compromised.
        b. As a result of the FBI's investigation it was determined that the break-ins were committed by a gang of teenagers that referred to themselves as the 414 Gang—likely a tribute to the area code from which they were committing their crimes.
        c. Results—In 1986, legislation was finally approved and termed the Computer Fraud and Abuse Act (CFAA).

i. Made the unauthorized access of a federal interest computer an illegal act.

ii. Only addressed hacking into federally controlled computers unless the incident occurred across two or more different states.

2. Late 1988—On November 2, 1988, Robert Morris, a Cornell University graduate student, inadvertently released a computer program that would come to be referred to as a worm program.

a. Morris gained extreme notoriety for being the first person charged under the CFAA; this recognition led to Morris being inducted into several hacker halls of fame.

b. Because of the unique circumstances surrounding the case of Robert Morris, the Cornell Commission was developed and charged with the dual task of investigating the incident and making recommendations on how to prevent future occurrences.

i. Morris's actions were indeed accidental in nature and as a result of his actions, several security deficiencies in the computer systems were detected.

ii. The worm program resulted in a positive change and improvement in computer security.

c. Morris was ultimately sentenced to three years probation, was fined $10,000, and was ordered to perform 400 hours of community service.

1. Late 1980s–early 1990s—As a teenager in the 1980s, Kevin Mitnick was constantly in trouble with authorities because of his inappropriate activities involving computers.
    a. In the early 1990s, however, Mitnick's name became very well known when he was tracked cross-country by a computer engineer whose computer Mitnick had illegally accessed.
    b. Mitnick became regarded as a serious criminal and holds the distinction of being the first computer-related criminal to be featured on the television show "America's Most Wanted."
    c. Mitnick is credited with bringing the issue of hacking to the forefront of the nation's attention and scaring the government into believing that hacking could be dangerous.
    d. Over the course of his criminal career, Mitnick managed to gain access to some of the most guarded computer systems in the country through a combination of computer programming skills and social engineering ability.
    e. As a result of his incarceration, Mitnick became arguably the world's most popular hacker.

IV. The Types of Hackers

A. There are generally four categories of hackers recognized in the hacker/cracker community: black-hat hackers, white-hat hackers, gray-hat hackers, and script kiddies.

B. In this work, there will be two additional types of hackers discussed: the hactivist and the cyberterrorist.

C. Black-hat Hackers

1. These are individuals who violate computer security for little reason beyond maliciousness or for personal gain.
2. Hackers write programs to damage computer systems and networks; the result is that computer security and anti-virus manufacturing have become full-time enterprises.

D. White-hat Hackers

1. Main objective is to provide computer security programs that will protect systems from being illegally and maliciously penetrated.
2. Hackers will still search out target computers and then attempt to hack into the systems, but once successful, they will normally cease their activities and alert the owner of the computer system to the vulnerability.

E. Gray-hat Hackers

1. These hackers are a combination of white-hat and black-hat hackers and are opportunistic.
2. Hackers will search target computers, gain access, notice the system's owner, but they will normally elect to offer to repair the defect for a small amount of money.
3. While this may appear to be a form of blackmail, in the business world such decisions may be a matter of cost-benefit analysis.
4. Recently, the practice has witnessed a decrease in use as more businesses have elected to prosecute individuals who attempt these acts.

F. Script Kiddies

1. Lowest level on the "hacking ladder," and may have little to no computer programming skills.
2. May not even be considered a hacker at all, given the average level of computer skill these individuals possess.
3. Script kiddies earn their names from their ability to surf the Internet looking for hacker utility programs and then launching the programs at a target computer system.
4. Most dangerous of the hackers because this individual has no idea how the program will affect the computer system the attack is being launched upon.

G. Hactivists

1. The hactivist is an individual who hacks as a means of spreading their political message.
2. The majority of hactivist attacks involve web page defacement, which refers to when a hacker gains access to the server that is storing a web page and then modifies the page to display their own message.

H. Cyberterrorist

1. Cyberterrorist refers to an individual who uses their hacking ability to instill a sense of fear into the public.
2. The cyberterrorist is one who would break into a computer system or network and then in some way manage to cause damage or death because of the loss of the service.

V. Hacker Technique and Modus Operandi

A. Many people are under the assumption that all activities related to hacking are conducted from the safety of their home and involves only the computer and the Internet.

B. Pre-hacking stage is defined as the process of using the physical techniques that precede the actual act of hacking into the computer.

1. Targeting is the first step in the pre-hack stage.
    a. Determine which computer system or network they will attack.
    b. Today, the method of selecting an actual company or network may involve one of two methods.
        i. May physically select a target that is of interest to them.
        ii. Use of a port scanner (software packages that scan computer networks to determine if any computers have open port settings).
            1. Because these open ports allow for information to pass into and out of computers, it is also a primary method for hackers to gain access to a computer; and, once the computer is controlled, the network is also available to the hacker.

1. The second stage of pre-hacking is known as the researching and information-gathering phase.
    a. Physically visit or contact the target in hopes of gaining information that will assist in penetrating the system.
    b. Researching will normally involve one of two different techniques.
        i. Use of social engineering, which may be employed when the hacker contacts the system administrator under the auspices of being a legitimate user who is locked out of the system.
        ii. Reverse social engineering, which is when the hacker will let the system administrator or a network user contact them for assistance.
        iii. Use of dumpster diving, which refers to the act of literally climbing inside a trash dumpster and searching for information that could be of benefit to the hacker when he or she attacks the computer network. .

D. Once the researching stage has been completed, the hacker will begin the actual hack of the computers or network.

1. The hacker will at this point attack the target using their hacker tool kit.
2. The hacker tool kit is a collection of software that a hacker will need to gain entry-level access.
    a. According to Dr. K., a self-proclaimed hacker and e-zine publisher from the United Kingdom, any hacker tool kit must contain the following items: password grabbers and key loggers, blue boxing programs, war dialers, encryption software, program password crackers, BIOS password crackers, security vulnerabilities scanners, packet sniffers, and UNIX vulnerabilities scanners.
    a. Password grabbers and key loggers
        i. Can be planted on a target computer and can run in the background without the computer owner's knowledge.
        ii. Installed on a computer as a means of recording each key that is pressed by the user of the target computer.

iii. Installed on a computer as a means of recording each key that is pressed by the user of the target computer to ensure that workers are not performing personal business on the company's time.

c. Blue boxing programs

i. Have been traditionally used in the hijacking of telephone services.

ii. Today, however, there are software programs that emulate the blue box and open phone lines.

iii. Interestingly enough, while there remains support for the use of these programs, and Internet message boards still contain discussions of the devices, many of today's telephone lines are not susceptible to attacks from these devices.

d. War-dialers

i. The term "war-dialer" refers to a program that will scan a predetermined range of phone numbers to determine if there is a computer enabled to receive telephone connections.

ii. More modern war-dialers, also sometimes referred to as demon dialers, will allow users to search for voicemail boxes, private branch exchanges (PBX), and other telephone services that could be of interest to users.

iii. Made famous by the movie *WarGames* in the 1980s.

i. A war-dialer program will provide its user with a list of numbers that successfully contacted computers.

ii. Once the list is provided to the hacker, then they will begin attempting to contact the numbers in order to determine if any of the computer systems are worth the effort associated with hacking into the system.

iii. These programs are not as useful today for at least two reasons: (1) they can be traced by telephone companies and (2) the majority of computers now connect to networks via Ethernet cables.

e. Encryption Software

i. Encryption software was originally designed for use by the government as a means of protecting files from being seen by those without proper security clearance.

ii. Phil Zimmerman, a computer programmer who determined that his encryption software should be available to the public, released a version of the software known as Pretty Good Privacy (PGP) free of charge.

iii. For simplicity's sake, it should be noted that encryption assigns new letters to represent the letters already in the file and will then scramble the letters to make interpretation significantly more difficult.

iv. As of late 2009, the encryption PGP platform is still considered by many to be one of best encryption programs available, but there are many software companies that have developed encryption software programs.

f. Password Recovery Software
    i. Password recovery software is used to satisfy one of the driving forces behind hacking motives—the belief that information should be free.
    ii. Normally consist of utilities designed to crack the internal passwords of programs such as Microsoft Word, Microsoft Excel, and other commercial software programs.
    iii. Program password attacks consist of either dictionary attacks, which cycle through entire dictionaries trying to break the password, or name attacks, which cycle through entire databases of names both forward and backward.
g. BIOS Password Crackers
    i. Designed to hack into the BIOS passwords stored on the motherboard of a computer.
    ii. BIOS password crackers are necessary to gain access to computers belonging to more sophisticated users.
    iii. Originally, these cracker programs were designed for legitimate uses such as when an individual purchased a used computer that contained a password stored on the motherboard.
    iv. Hackers, however, have since turned these utility programs into a means of gaining unauthorized access to personal computers.
h. Security Vulnerability Scanners
    i. Security vulnerability scanners are programs that have little purpose beyond scanning a network to determine whether there are known security vulnerabilities present in the network that have been reported in the database.
i. Packer Sniffer
    i. A packet sniffer program is computer software designed to sniff packets of data as the information is moved across a network.
    ii. A packet sniffer is installed on a network and programmed to examine all packets that pass through the network and are used by individuals attempting to steal passwords or credit card information from commercial websites.
j. Operating System Password Crackers
    i. Similar to password-cracking programs designed for software programs, but are designed to crack passwords on the various operating systems.
    ii. The programs are operating system specific, meaning that a password cracker for the Windows operating system will not normally crack passwords on the UNIX/Linux operating system.
k. War-Driver Programs (Wireless Network Scanners)
    i. Refers to the process of driving around looking for wireless networks that are not secured.
    ii. Some war-drivers claim that war-driving refers only to the locating of wireless networks and that individuals who actually

gain access to the wireless networks are said to be "piggybacking" and may possibly be in violation of the law.

E. Hacker Attack Techniques

1. There are several different types of attacks used by hackers once they have access to a system.

2. In the early 1990s, Peter Denning referred to many of these attacks as crimoids, which he considered a crime that used creatively applied technology and received extensive coverage in the news media.

3. The more commonly encountered of Denning's crimoids that are still discussed today are: data manipulation, Trojan horses, and viruses.

a. Data Manipulation

i. Refers to the process by which an individual changes data or deletes data from a computer system as a means of causing harm (almost always financial) to the computer's owner.

ii. Situations in which these attacks are used:

1. Hacker gain access to a reputable computer software company and destroy any existing research on an upcoming software system.
2. Former worker uses their security codes to gain access to bank records and then transfers funds into a personal account.

iii. It is believed that the majority of cases involving this technique are inside jobs committed by angry personnel.

b. Trojan Horse

i. The Trojan horse attack is so named because the instructions for the program are secretly inserted onto a computer system or network without the owner's knowledge and in much the same manner that Greek warriors sneaked inside the city of Troy using a wooden horse.

ii. Are commonly sent to a target computer system via e-mails to legitimate users of the system.

iii. A hacker may enjoy releasing a Trojan horse onto a computer system for a number of reasons.

1.To sabotage the computer network in order to gain access to other computers on the network.

2. To see how the introduction of additional programs will affect the entire system's operations.

iv. Not used as frequently today, is that of the time bomb, which is occasionally referred to as a logic bomb.

1. Unlike the normal Trojan horse program, however, the logic bomb is designed for damage and sabotage.

2. Can be set to activate on a specific date, time, or condition.

3. The time bomb program is rarely read about today and is most encountered in situations when an individual desiring

revenge against a company or individual uses the program to seek retribution

c. Computer Viruses

i. Any computer program capable of damaging a victim's computer and the program is replicable.

ii. Viruses are quite possibly the biggest and most expensive problem facing computer users today.

iii. The leading anti-virus computer software manufacturers, Norton and McAfee, now maintain a team of anti-virus computer programmers whose job consists of analyzing emerging threats and writing anti-code to prevent infection of subscribers' computers and networks.

iv. One of the more common targets for a computer virus is the boot sector of the target computer's hard drive.

v. Viruses are deposited on the boot sector so that each time the computer is booted up the virus will load itself and run its program.

d. Denial of Service Attacks

i. Refers to an attack in which an Internet website or network server is flooded with enormous amounts of data that in essence consumes all resources of the target computer system.

ii. Result in the target computer crashing or shutting down

iii. Goal is to prevent legitimate users from accessing the computer

iv. Advances in computer technology have resulted in computer systems today that are able to handle larger amounts of data requests.

1. These advances, along with the development of administrative settings that now allow network administrators to limit the number requests being accepted from the same computer, have resulted in better protections from these attacks.

2. As a result there is a growing trend toward the use of dDOS attacks—distributed denial of service attacks

a. allow for multiple computers to launch data at a target computer system; thereby allowing for a heavier flood of data that can shut down the more powerful computers

b. The dDOS software can be installed on a computer or network without the system administrator's permission and may shut down its desired target before many individuals realized their computer has been used in a denial of service attack.

e. IP Spoofing

i. IP spoofing refers to the process of forging a computer's Internet protocol (IP) address.

ii. Reasons an individual will attempt to accomplish this activity:

a. Send out massive amounts of electronic mail.
b. Used by spammers.

f. Web Spoofing

i. The act of web spoofing involves the redirection of a user's Internet browser to a given website when the user types in a similar URL address.

ii. Once within the grip of these sites it is sometimes hard to back out because of the sheer number of pop-up ads that launch upon the initial accessing of the website.

iii. The technique is especially popular when used in conjunction with an e-mail scam whereby an individual will receive an e-mail telling them to visit their bank's website to update their information.

iv. Web spoofing should not be confused with cyber squatting, which was for a while a very popular form of Internet deception.

v. Cyber squatting—An individual will wait until an official website neglects to renew their annual registration for the domain name, and then they will purchase the domain and begin putting in their own information.

g. Non-Software/Non-Network Based Attacks

i. There are additional acts that are involved in the act of hacking, but they are less dependent upon computer software to be accomplished.

1. Piggybacking—Refers to the process whereby an individual gains access to a computer by following someone into a secured room.

2. Electronic piggybacking—Involves the illegal user waiting until a legitimate user neglects to sign off and then taking control of their account.

VI. The Crime of Phreaking

A. Phreaking refers to one of the oldest computer crimes around—theft of telecommunications service.
B. The "ph" is used in place of the "f" to represent the phreaker's tool of choice, the telephone.
C. Today, the term "phreaking" refers to any activity resulting in the individual gaining use of a telecommunications service without paying for such services.
D. Phreaking may be commonly encountered when a telephone subscriber receives his or her bill and there is an abundance of calls not made by the subscriber.
E. John Draper was one of the more famous and influential phone phreakers of all time when he earned the nickname Captain Crunch by opening telephone lines through the use of a whistle he obtained from a cereal box.

1. Steve Jobs and Kevin Poulsen were two of the better known phone phreakers to be influenced by Draper.

2. Jobs was a co-founder of Apple Computers. Before he was a computer entrepreneur, however, he made his living in college selling blue boxes, which

were the small electrical devices that emitted a tone capable of controlling early telephone lines.

3. Kevin Poulsen spent the majority of his early life in trouble with the law because of his activities, which included breaking into telephone companies for manuals and training materials for insight into how the company's main computer worked and tapping into telephone lines and monitoring conversations.

F. How Phreakers Operate

1. Today, there are computer programs written to recreate the tones and activities of many phreaking activities.

a. There remain individuals who employ other methods, such as phreak boxes, whose functions are discernable by its color.

i. Aqua box—designed to prevent the proper application of a Lock-in-Trace device, which is a device that generates sufficient electricity to hold open a phone line after the call has ended but before the call has been traced.

ii. Beige box—used as means of listening in on other people's phone conversations or making free long-distance phone calls at someone else's expense.

iii. Red box—used to replicate the sounds made by coins when they are dropped into a pay phone.

iv. Blue box—used to replicate the 2600-megahertz tone used to open telephone lines.

v. Rainbow box—used to generate electricity through the telephone system and is normally used as a means of damaging an adversary's phone system.

2. Many of the phone phreaking devices have seen a decreased level of use attributable to the advances in telecommunications that have outdated the devices.

3. Phreakers are now looking toward digital techniques and new creative applications for phreaking abilities.

G. Cellular Phone Phreaking

1. When a cellular telephone is first activated it is assigned an Electronic Serial Number (ESN) and a Mobile Identification Number (MIN), which are used by the cellular provider to direct any incoming phone calls.

a. Using a radio scanner and a data-capture tool, the phreaker will capture the ESN and MIN numbers and reprogram their cellular telephone using the stolen numbers.

b. Any calls made using the stolen information will be billed to the registered owner of the numbers.

2. Another area of cellular phone phreaking involves accessing a person's cellular telephone via the BlueTooth connection that many phones utilize to connect cellular phones with wireless earpieces; this technique is used to intercept future telephone calls or modify address books.

H. Calling Card Fraud

1. Calling card numbers are stolen from unsuspecting consumers via any number of different techniques such as shoulder surfing or the use of calling card generators

I. Call Sell Services

1. The call sell service involves the use of traditional phreaking activities, calling card fraud, and cellular phone cloning.

2. Phreakers will charge individuals anywhere from $5 to $15 for the unlimited use of a telephone system.

J. Phreaking is commonly encountered in serious hacking cases and in organized crime operations because of the ability to allow these individuals to hide their true identity and the location.

VII. The Hacker/Phreaker Subculture

A. Previous research attempted to classify hackers and phreakers into distinct traits, but the wide-scale availability of the Internet makes it difficult to classify these individuals.

B. The Hacker Ethic

1. There are many individuals who violate computer systems but do so without removing any data from the system or causing any damage to the system.

2. To a hacker there is no such thing as secured information.

3. The majority of hackers also appear to believe that information should not be secure.

4. Hackers value the creation of something great far more than they value the destruction or damage of a computer system.

C. Hacker Language

1. Difference in hacker language and acceptable English

a. Spelling

i. Have great respect for what was once a required tool of their trade, the telephone and the modem (will replace "f" with "ph" in words).

ii. Numbers are routinely replaced with letters and letters replaced with numbers.

b. Sentence Formation

i. Routinely type in all caps.

ii. Will repeat an expression for emphasis.

iii. Will shorten unimportant expressions.

iv. Will use asterisks around a word to indicate an expression.

2. Basic terms used by hackers:

a. Neophyte or newbie—an individual who is new to hacking and phreaking.

b. Suit—law enforcement officer.

c. Lamer—an individual who thinks he or she is a real hacker when he or she is really just a beginner or copycat.

d. Leech—an individual in an IRC chat that is not sharing files or information with others.

D. Hacker Conferences

1. One of the more famous conventions is that of DEFCON, which is held in Las Vegas, Nevada, every summer, and brings together the very best and brightest of the hacking and phreaking community to discuss the latest developments and techniques in the hacking community.

2. Many computer security professionals and federal law enforcement personnel will also attend to learn the latest tricks and techniques, but federal law enforcement personnel are received warmly.
3. Why do people attend these conferences?
    a. They are curious about computer security and want to learn about topic.
    b. Companies want to scout out potential employees.

VIII. Conclusion

Key Terms

BIOS password crackers: Utility programs that are designed to hack into the BIOS password stored on the motherboard of a computer.

Black hat hackers: Individuals who violate computer security for little reason beyond maliciousness or for personal gain.

Blue box programs: Used in the hijacking of telephone services.

Call sell services: An operation in which phreakers will charge individuals anywhere from $5 to $15 for the unlimited use of a telephone system.

Calling card fraud: Stealing the calling card numbers from unsuspecting consumers.

Cellular phone phreaking: A process designed to reprogram cellular telephones using the illegally obtained Electronic Service Number (ESN) and Mobile Identification Number (MIN) of the registered owner of the numbers or by accessing a person's cellular telephone using their BlueTooth connection to intercept future calls or modify the phone's address book.

Computer virus: Any computer program capable of damaging a victim's computer that is replicable.

Cracker: One who violates software copyright protections and gains inappropriate access to password protected files and services.

Crimoid: A crime that creatively applied technology and received extensive coverage in the news media.

Cyber squatting: When an individual waits until an official website neglects to renew their annual registration for the domain names, purchases the domain name, and begins putting in their own information.

Cyber terrorist: An individual who uses their hacking ability to instill a sense of fear into the public.

Data manipulation: The process by which an individual changes data or deletes data from a computer system as a means of causing harm to the computer's owner.

Denial of service (DOS) attack: An attack in which an Internet website or network server is flooded with enormous amounts of data that in essence consumes all resources of the target computer system.

Dictionary attack: An attack on the internal password of programs that cycle through entire dictionaries trying to break the password.

Distributed denial of service (dDOS) attack: An attack that allows for multiple computers to launch data at a target computer system, allowing for heavier flood of data that can shut down the more powerful computers.

Dumpster diving: The act of literally climbing inside a trash dumpster and searching for information that could be of benefit to the hacker when he or she attacks the computer network.

Electronic piggybacking: The process whereby an illegal user waits until a legitimate users neglects to sign off and then takes controls of the person's account.

Encryption software: Software designed to protect files from being seen by those without proper security clearance.

Gray-hat hackers: Individuals who gain access to a computer system and offer to repair the defects in the system for a small fee.

Hacker: An individual who uses their personal computers to gain unauthorized access to other individuals' and businesses' computers.

Hacker tool kit: Collection of software that a hacker will need to gain entry-level access.

Hactivists: Individuals who hack as a means of spreading their political message.

IP spoofing: The process of forging a computer's Internet protocol (IP) address.

Name attack: An attack on the internal password of programs that cycle through entire databases of names forwards and backwards.

Operating system password crackers: Programs designed to crack passwords on the various operating systems.

Packet sniffing: Computer software designed to sniff packets of data as the information is moved across a network.

Password grabbers and loggers: Programs that are installed on a target computer as a means of recording each key that is pressed by the user of the target computer.

Password recovery software: Utilities designed to crack the internal passwords of programs.

Phreaking: Any activity resulting in the individual gaining use of a telecommunication service without paying for such service.

Physical piggybacking: The process whereby an individual gains access to a computer by following someone into a secure room.

Port: The opening through which the computer receives data via the network.

Port scanners: Software packages that scan computer networks to determine if any computers have open port settings.

Pre-hacking stage: A term used to describe the process of using the physical techniques that precede the actual act of hacking into the computer.

Reverse social engineering: Process by which the hacker will let the system administrator contact them for assistance.

Root access: Term sometimes used to describe higher-level access into a computer or network.

Script kiddies: Individuals who surf the Internet looking for hacker utility programs and then launch the programs at a target computer system.

Security vulnerability scanners: Programs that have little purpose beyond scanning a network to determine whether there are known security vulnerabilities present in the network that have been reported in the database.

Social engineering: An ability to use written and verbal communication skills to trick individuals into providing necessary information.

Time bomb (or logic bomb)- Program that is secretly inserted on the network or operating system designed for damage or sabotage.

Trojan horse: An attack in which the instructions for the program are secretly inserted onto a computer system or network without the owner's knowledge.

War-dialer: A program that will scan a predetermined range of phone numbers to determine if there is a computer enabled to receive telephone connections.

War driving: The process of driving around looking for wireless networks that are not secure.

Web spoofing: The redirection of a user's Internet browser to a given website when the user types in a similar URL address.

White-hat hackers: Individuals who provide computer security programs that will protect systems from being illegally or maliciously penetrated.