Understanding Hackers and How They Attack

Why should you concern yourself with the motivations and lifestyles of computer hackers? This understanding will help you to “know the enemy” and prepare a better defense. Understanding the different types of hackers and their motivations will help you know what kind of information to protect and whom you have to watch. Ideally, you should protect all of your organization’s information, but this is often not possible for practical or financial reasons. This chapter describes who hackers are, how they attack, and where they target. Remember, a hacker can be the teenager you saw under arrest on TV last night, or the person in the next cube. This chapter will provide the foundation you need to make informed decisions about your organization’s computer security.
Chapter at a Glance

This chapter helps you to do the following:

- Become familiar with the common hacking terminology
- Become aware of the different motivations for cybercrime
- Understand the different types of attacks
- Be conscious of typical hacking targets
- Know who to watch internally and externally

Types of Hackers

A *hacker* is an individual who has a great deal of technical knowledge about computer systems and their security. Originally, the term had no negative connotations; in fact, it indicated an individual with a great deal of technical prowess. Today the term frequently refers to cybercriminals. The following classified ad lists the profile of a typical criminal computer hacker:

<table>
<thead>
<tr>
<th>Help Wanted</th>
<th>Computer Hacker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Black Hat hacking organization looking for new recruits. Ideal candidate will be talented, obsessive, and organized. Morals and ethics negotiable. Under 25 years old preferred.</td>
<td></td>
</tr>
</tbody>
</table>

Hacking has its roots in the computer culture of the 1950s and 1960s when access to computers was extremely limited and expensive. The timesharing of large mainframe computers was tightly controlled and many individuals who wanted to increase their knowledge and technical abilities found alternate ways to gain entry. Out of these roots has grown a full spectrum of hackers from the true law-abiding security expert to the computer criminal.

The general term “hacker” can be broken down into five distinct groups. These categories help define the type of individual and the threat that they present. These terms attempt to categorize human motives and behaviors; they are not absolutes. They provide a way to discuss different types of hackers and understand what type of actions attackers are likely to take against your organization. This allows you
to strategically implement security in the areas that are the most vulnerable to attack.

**The White Hat Hacker**

The “good guys,” often security professionals, are called *White Hat hackers*. They stay entirely within the law, only access systems with permission, and work to identify and fix security flaws. If they find security problems of a particular product, they inform the vendor so that it can be fixed. They do not publicize the problem.

White Hat hackers often work as security professionals, using the hacker tools to test the security on their own systems. They also closely monitor Internet resources that discuss hacking, vulnerabilities, and attacks. They may also attend hacker conventions and subscribe to hacker publications. Like an undercover police officer, they sometimes walk a fine line.

*Samurai hackers* are White Hat hackers that consult as security professionals. They are usually privy to the highest level of access and have an in-depth knowledge of a company’s security vulnerabilities, and consequently, they must have extremely high ethical standards. Some companies hire reformed hackers who gained their knowledge in less reputable activities. This is the equivalent of hiring an ex-burglar as a physical security expert and is a risky practice.

**The Ethical or Gray Hat Hacker**

Hackers who find security holes and report them are known as *Ethical or Gray Hat hackers*. Sometimes they give the company a chance to fix the problem before publicly posting it. Others do not; they immediately publish the problem, allowing malicious hackers the opportunity to exploit it. Many also break into systems without permission. They believe they are providing a service to consumers by forcing companies to provide better security and products.

Tom Cervenka considers himself an Ethical hacker. He discovered a weakness in eBay’s security that allows the theft of users’ identities. He claims he notified their tech support and that they failed to act. He then publicly posted a step-by-step guide to exploiting the weakness on the Internet. He feels his actions are justifiable because it forced the company to act. eBay feels differently about this being an “ethical” act.

An attack by an Ethical hacker is obviously better than one by someone with malicious intent. However, when you are under attack it is impossible to tell the intent until it is too late. Therefore, the IT
resources must scramble to protect information and record the attack as if it was malicious. If the press reports the attack, public confidence is undermined, especially if the organization deals with financial or confidential information. The public may be relieved the attack was benign but this may not stop them from moving their business to a company with a better security record.

The Script Kiddie

Unskilled hackers who use tools written by more experienced hackers are called Script Kiddies. They are typically teenagers seeking the thrill of publicity. They may gain access to systems, disrupt systems, or deface web pages. They are easier to detect and catch but their attacks can still be very damaging. It can be very embarrassing for a company to have their security thwarted by a 14-year-old boy on his Dad’s old 486 PC. Script Kiddies have a great deal of free time, often work in groups, and make great headlines.

In the first quarter of 2000, major online companies including CNN, Amazon, Yahoo!, Excite, and eBay experienced Denial of Service attacks. These attacks sent huge amounts of traffic to the websites until they could no longer handle the volume. Regular customers experienced a denial of service when they attempted to conduct legitimate business on the website. Ironically, the alleged perpetrator, alias Mafiaboy, was a 15-year-old Canadian Script Kiddie.

The Hacktivist

A Hacktivist uses computer knowledge to promote a political or social cause. They may be novices or sophisticated hackers. A company can be the target of this type of hacker if it has controversial business practices, technology, or customers. For instance, the British banking giant, HSBC, experienced the defacement of four of its websites. The hacker, alias Herbless, did this to protest the fuel prices in the United Kingdom. His defacement included an activist statement and guidelines for other Hacktivists. He even posted the following note for the system administrator:

Note to the administrator: You should really enforce stronger passwords. I cracked 75% of your NT accounts in 16 seconds on my SMP Linux box. Please note the only thing changed on this server is your index page, which has been backed up. Nothing else has been altered.
The Cracker or Black Hat Hacker

Hackers who use their knowledge to commit crimes have been dubbed Crackers or Black Hat hackers. These crimes can include vandalism, destruction of property, fraud, theft, corporate or government espionage, and terrorism. They are aware that what they are doing is illegal, and consequently, they attempt to enter systems undetected and leave as little evidence behind as possible. This makes them the most challenging hackers to detect or catch.

The Phonemasters was a group of 11 Black Hat hackers that gained access to telephone networks of companies including AT&T, GTE, MCI WorldCom, Southwestern Bell, and Sprint. They broke into the Equifax and TRW credit-reporting databases. They entered the Lexis-Nexis databases and the systems of Dun & Bradstreet. Incredibly, they had access to portions of the national power grid and air-traffic-control systems. They also hacked their way into a collection of unpublished telephone numbers at the White House. According to FBI estimates, the group was responsible for approximately $1.85 million in business losses.

The Hacker Culture

There are as many reasons for hacking as there are types of hackers. Hacking has its own culture with a unique language, code of ethics, heroes and villains, and competing gangs. Hackers have group organizations, conventions, printed and electronic publications, and even a Hacker Anti-Defamation League.

Within the hacker culture, knowledge is power, and an Elite hacker is an individual with great technical proficiency. This often comes from hours of practice, often using unauthorized access on someone else’s computer network. The hacker ethic varies but most believe that information and computer access should be freely shared. Many also believe that cracking into systems is ethical as long no harm is done.

The average hacker is a 14- to 28-year-old white male. A hacker is often an intelligent, academic underachiever who is a student or employed in a technical field. Like any profile, this is a broad generalization and the diversity is increasing. Hackers are not known for their conformity and the cultural distinctions vary from group to group. In fact, these distinctions can be helpful when trying to catch or prosecute a hacker because these differences often leave clues to the hacker’s identity.
Many hackers go by distinctive aliases and use Internet relay channel (IRC) to plan or boast about their exploits. They use hacker slang and techno speak to create their own language. This language has its own conventions for spelling, syntax, punctuation, and capitalization. For example:

Rd00ze: One code monkey wedge wedge his new gonkulator and boy is the suit mad. Lamer can't reload windoze. Stupitude. <HHOS>

Roughly translated:
A guy who works as a low-level programmer broke his pretentious new computer and his boss is mad. He doesn’t know how to reload Microsoft Windows. The speaker, alias Rd00ze, thinks the programmer is stupid and is, ha ha, only serious.

Hacker slang, aliases, and group associations can help the authorities identify a hacker. Script Kiddies often leave messages in hacker slang and sign their work with their aliases. They also develop patterns of attack, such as repeatedly using the same tool or process. Not all hackers participate in the hacker culture; some are loners or consider the activities beneath them. However, all hackers have a modus operandi, and it is wise to collect as many clues as possible.

The Motivations of a Hacker

A major motivation among hackers is status. The bigger the target, the more sophisticated the attack, the more status the hacker gains. As previously mentioned, hackers label their heroes Elite hackers. This requires them to reach a certain level of knowledge and then demonstrate it to their peers. The media attention also provides acknowledgment and attention, increasing their status.

The websites of government agencies and large corporations are common targets. These targets gain a great deal of attention and status in some hacking circles. In 1996, hackers defaced the Central Intelligence Agency (CIA) web page changing the title to Central Stupidity Agency and modified an Air Force web page to include pornographic images. In October 2000, a young Cracker attacked and defaced more than 10 government sites including White Sands Missile Range, Hanford Nuclear Reservation, and the Department of Veterans Affairs. The list of government pages defaced or disabled is long and distinguished.
The young Cracker (he gives his age as under 16) that hit in October 2000 did not limit his work to government sites; he also went after the ultimate corporate site, Microsoft. Microsoft is a high-priority target for hackers because of its market dominance and controversial business practices. The Cracker defaced several of the sites by leaving love notes written in hacker slang. He claims he used hacking to escape the reality of his personal problems.

Less than a week later, a Dutch hacker also cracked Microsoft systems. He claimed to have been able to alter files available on its download site. He added a boast of his victory in the form of a text file, but claims he could have added a destructive file to customer downloads. After his attack, Microsoft quickly patched the known security flaws on its servers. He states his reason for the attack was to expose security flaws. Many hackers, especially White and Gray Hat, name this as their motivation.

Financial gain can also motivate Crackers. Credit card fraud and illegal wire transfers are the usual ways to use hacking to increase wealth. Some hackers feel that it is acceptable to emulate Robin Hood and steal from large, wealthy companies giving the money to a good cause. Others skip the rationalization and use it for their own personal gain.

In August 1994, Vladimir Levin, a Russian computer programmer, transferred millions of dollars out of Citibank accounts. He was part of a complicated scheme of wire transfers and pick-ups that moved money out of Citibank to accounts all over the globe. He claimed his salary from St Petersburg’s Technological Institute was so low that he had to steal the money.

Corporate or government espionage also motivates some Crackers. They steal intellectual property, trade and military secrets, and other desirable information. They use the information for their own purposes, or sell it to interested parties. Several members of the infamous West German hacking group, the Chaos Club, collected information about military installations and technologies and then sold it to the KGB. Clifford Stoll, a persistent systems administrator at the Lawrence Livermore National Lab in Berkeley, led the effort to track them down.

Political and activist goals are relatively new to the hacking community, but they are becoming more common. A company may become a target because of its use of controversial medical technology, genetic engineering, or disregard for the environment. A law firm representing a controversial client can be a prime target. Hacktivists target and disable or deface sites that represent the views that they oppose.
The December 1999 World Trade Organization (WTO) Conference in Seattle was the scene of both street and cyberprotesting. Hacktivists disabled the WTO conference website for an entire day and slowed it to a crawl during most of the conference. They also made an unsuccessful attempt at defacing the site.

Israeli and Palestinian sympathizers have hacking as a weapon of war. During October–November 2000 this hacking escalated from political, to criminal, to terrorist. The attack began with the defacement and disabling of more than 30 sites. Palestinian-affiliated hackers then publicly posted the personal information of the American Israeli Public Affairs Committee members. Israeli supporters then retaliated by posting Palestinian leaders’ cell phone numbers, information about accessing the telephone and fax systems of the Palestinian Authority, 15 Internet relay channels (IRCs), and an IRC server through which the Palestinian movement communicates. Several U.S. companies were also attacked. This included the Israeli Public Affairs Committee and Lucent, which has business interests in Israel.

Personal revenge can motivate current or former employees to hack. This is a growing problem for organizations; some polls claim that approximately two-thirds of network security breaches come from inside the company. These attacks can range from embarrassing to devastating. The employee turned hacker may inadvertently crash a system or intentionally destroy information. Building a hackproof wall to the outside world is not enough, security plans must also include inside policies and protections.

Eastman Kodak charged Chung-Yuh Soong, a former employee, with transmitting highly confidential software files to a competitor in California. The only reason they detected the alleged theft was that the document was so large it crashed the server. At Pixar Animation Studios, the entire company received an email listing the salary of every employee. The email seemed to originate from CEO Steve Job’s address. Although he did not send it, evidence does point to a current or former employee. These are just two examples of inside jobs that put organizations at risk.

**Hacker’s Toolkit**

There are many tools in the hacker’s toolkit. These tools include technical and non-technical techniques that allow them to gain access to systems and successfully complete the goal of the hack. This section
provides an overview of these tools and their uses. The upcoming chapters describe these tools in detail and include recommendations for tools and policies that will help prevent their successful use.

Hackers have their favorite tools and each computer system has its unique strengths and weaknesses. Nevertheless, most attacks follow a general pattern that include the following steps:

1. Gather information. Hackers gather both technical and general information. This includes names and telephone numbers of technical staff, network operating systems, security practices, remote access dial-up numbers, and passwords.

2. Gain initial system access. During this step a hacker enters the target network, often with limited access and rights.

3. Once he has opened the door, the hacker begins exploiting the system weaknesses to increase the level of privilege and expand access. He works to gain superuser or administrative status that will gain him full access. He may achieve this on the first attack, or he may use a series of attacks to gradually increase his privileges.

4. Carry out purpose of the attack. This step varies depending on the hacker’s goals. A White Hat working on behalf of the company would identify the weaknesses, fix them if possible, and then leave. A Cracker could begin copying files to steal information, installing a destructive Trojan program, or other malicious activities.

5. Install back doors. A hacker may tamper with the system and build an easy entrance for a return trip.

6. Cover tracks and exit. Hackers usually attempt to clean up after themselves and remove all traces of their attack. This involves modifying log files that record access and system changes.

The hackers use numerous techniques during these steps. One technique, phreaking, is any intentional misuse of the telephone system. It originated as a way to gain free phone access or crack into phone systems and disrupt them. Some hackers started as phreakers and use these techniques to gather information, cover their tracks, or cause additional damage to an organization’s communication systems.
Once hackers have cracked into a phone system they may monitor voicemail or temporarily forward phone calls to a number that they control. Hackers have used this ability to temporarily act as a computer help desk, convincing unsuspecting users to provide them with user names, passwords, and other information. They have also monitored the voicemail of the technical staff, learning more about their system’s vulnerabilities, network configurations, access rights, user names, and passwords.

Hackers also use phreaking to cover their tracks. They frequently access systems through a dial-up modem and they do not want a traceable telephone number recorded in the system. They use their telecommunications expertise to dial in using numbers that do not belong to them, avoiding phone charges, and hiding their identities. A 75-cent phone bill discrepancy caught by an observant systems administrator led to the detection and eventual arrest of the Chaos Club members.

Another telephone activity is war dialing also known as brute-force dialing. These tools dial a sequence of numbers in order to detect modem tones. Telephone companies can easily detect the more primitive of these programs, but the more sophisticated dialers randomize the timing and sequence of calls. This makes them more difficult to detect and prevent. Once the dialer finds a modem it will attempt to log in using a series of passwords. If successful, the hacker gains initial access to the network.

Social engineering takes advantage of human weaknesses to gain access to passwords other information. Typically, a hacker will call up an individual and pose as technical staff. He will have usually gained enough company information to sound credible and the victim will often provide user name, password, or other vital information.

Recently, there has been a rash of social engineering involving email. The email, which appears to be from the site administrator, instructs the recipient to run a previously installed test program. The program then prompts the user to enter her password. The program then emails the password to a remote site and the hacker retrieves it. The following is a sample of this type of message:

OmniCore is experimenting an online high-resolution graphics display on the UNIX BSD 4.3 system and its derivatives. But, we need your help in testing our new product - TurboTetris. So, if you are not too busy, please try out the tetris game in your machine’s /tmp directory. just type:
/tmp/ttetris
Because of the graphics handling and screen reinitialization, you will be prompted to log on again. Please do so, and use your real password. Thank you for your support. You'll be hearing from us soon!

OmniCore

Social engineering is an incredibly effective way of gathering information. The creativity of the hacker and the security awareness of the potential victim are its only limits. There is story after story of hackers gaining vital information with just a simple phone call or email. Is it any wonder that this can occur in a society with naïve and trusting people? The same individual who purchases a faux pearl necklace or waits for Ed McMann to show up with a sweepstakes check will cheerfully provide a password.

While social engineering takes a smooth tongue and sharp mind, another technique, _trashing_, requires less glamorous skills. Trashing is the practice of going through rubbish to find information. This information can include account names, passwords, credit card numbers, and other security information. It is most effective near a computer help desk, Internet service provider (ISP), or network operation center. Although it is a risky, clandestine process, it can provide valuable information.

Another method of obtaining passwords is _password cracking_. There are password-cracking programs available for free on the Internet. These programs contain large dictionaries and try to guess passwords by trying each word. The more sophisticated programs include all possible alphanumeric combinations. These programs may be run against an individual account, system account, or against the actual password file that contains all of the users’ passwords. There is no guaranteed safe password because of these tools. However, the combination of a good network and password policies can prevent a hacker from successfully using these tools. The password security section in Chapter 7 outlines these policies.

_Packet sniffing_, another technical tool, captures user names and passwords by listening to data transmissions. It is essentially a wiretap applied to a network, analyzing each packet of information and extracting the relevant data. Many organizations install system tools designed to help manage the network. While these tools are very useful, they can allow hackers to install remote sniffing programs. In addition to capturing passwords, hackers can use packet sniffers to read email, data files, and financial information.
Pinging and port scanning are other technical tools that help gather information about computer systems. Network administrators use these tools and so do hackers. The ping utility sends a packet from the hacker’s computer to the target computer. If the computer is on and connected it will respond. Port scanning is a means of finding exploitable communication channels. The hacker then uses this port to gain entry to the system. Hackers can use both of these utilities to gather information, or to actually attack and crash systems.

IP-spoofing is the creation of packets using somebody else’s address. Hackers use this to hide their location and avoid identification. Crackers use spoofing in combination with various hijacking and flooding techniques to maliciously attack systems. Once hackers spoof their way in, they establish trust and then hijack a legitimate user connection. Then they proceed with an attack. Crackers also combine spoofing with floods of fake requests that eventually disable the system.

Another hacker activity is writing malicious code, including viruses, Trojans, and worms. These are covered in depth in Chapter 2. Virus writers may not consider themselves hackers, but they certainly fit the definition. They are individuals with a great deal of technical knowledge about computer systems and their security. They need this knowledge in order to create successful malicious code. Hackers use viruses and other malicious code to attack or damage individual targets or release them “into the wild” where they have the potential to attack random targets.

Depending on their background and motivation, hackers may use one or a combination of these tools. They may specialize and be very good at one technique or be jacks-of-all-trades. The modus operandi, or method of working, is one of the factors used to identify and apprehend cybercriminals. This book covers each of these tools and the results in depth.

Security Best Practices

The security checklist in the Introduction of this book points out the computer security areas within your organization that are the most critical to you. The following action steps will continue this process and give you a clear picture of the current state of computer security in your organization. This will help you get all the relevant information in one place and allow you to create a baseline to measure against as you make improvements.
This groundwork cannot be done overnight, it will take some time. So, set the process in motion now, and continue to work through the priority chapters you established in the Introduction.

Some of these actions you may not be able to personally accomplish. They may be outside your direct control, or you may not have the time. Depending on your position and organizational culture, pick one of the following approaches:

**Team** The team approach requires you to charter a cross-functional team. This team will work together through the chapters, analyzing and creating a strong but workable computer security culture within your organization. This plan is best because you get buy-in from different departments, better synergy, and creative ideas. However, it can take longer and requires good team dynamics. It is particularly effective in organizations where the staff regularly works in teams. It is also critical to make sure you have representatives from the key areas including IT, security, and HR. You don’t want to make the team too large; 6–8 people is ideal. They may not have expertise in all areas, so they will need to interview other people who do.

**Top-down** Use the top-down approach if you are in the position to bring in the appropriate department heads and have them review and analyze their areas. Have each complete the risk identification form and review their assigned area. Then have the report collated and provide the results to participants. Have them provide suggestions for improvement in their areas, using the guidance from the following chapters. You must be careful to approach it in a way that doesn’t put them on the defensive or you won’t get real information.

An alternate top-down approach is to work with an expert. If you have a computer security expert on staff or can bring one in temporarily or permanently, this is a good approach. Have them work through the process with you. They may have the computer security knowledge, but you have the leadership, support, and business knowledge that they need to be effective.

**Bottom-up** If you are not in a position to use the team or top-down approach then you can work from the bottom up. This means you gather and analyze the information, complete the risk identification form, and use the following chapters of this book
to prepare a proposed strategy. This will only be a start, because you may not have the knowledge or access to all the critical information. Depending on your position and organization, you could then provide this to the department heads, the CEO, and the IT manager. You must remember your goal to improve the organization’s computer security and minimize the risks. Therefore, you must deliver it the right people in a way that will get their buy in and cooperation.

**Best Practice Action Steps for Organizations**

- Gather and review computer security policies. What do you have in place? Are they readily accessible? Are they followed?

- Complete the Risk Analysis form provided in Appendix B. Don’t forget databases, email, customer lists, intellectual property, or financial data. This is an exercise in controlled paranoia; you will create action plans later. You may not know the answer to every question; if so, highlight this area and move on.

- Gather and review the computer security–training plan for both IT staff and the computer user community.

- Gather and review hiring policies. You may or may not be able to change them, but at least be aware of the risks if they exist. Examine contractors’ arrangements. Review reference and background check procedures, as well as the interview process. Finally, investigate security awareness.

- Gather and review physical security policies.

**Best Practice Action Steps for the Small or Home Office**

- Review your computer security policies. In a small or home office these may not be in writing, but what are your practices? Having only one computer system with all your data on it can leave you even more vulnerable than a large organization.

- Complete the Risk Analysis form provided in Appendix B. Don’t forget databases, email, customer lists, intellectual property, or financial data. This is an exercise in controlled paranoia; you will
create action plans later. You may not know the answer to every question; if so, highlight this area and move on.

- If you feel that your computer security leaves you at risk, consider bringing in a consultant to help you set up a more secure system. In a small or home office this makes much more sense than trying to become an expert on your own and taking time away from your core competency work. Working through the rest of this book will prepare you to effectively work with a consultant.

- Review your hiring policies. Do you use subcontractors or send work out? Do you do reference checks or background checks when warranted?

- Consider your physical security. Would it be easy to break into your house or office and remove critical data? What would be the results?