CHAPTER

2

Cyber Threatscape

INFORMATION IN THIS CHAPTER

- How did We Get Here?
- Attack Methodology With the Tools and Techniques Used to Execute Them
- Attackers (Major Categories of Threats)
- Defense in Depth—How Organizations Defend Today (Defensive Mountain Range)
- What the Threat is After (What We Should Focus on Defending)

HOW DID WE GET HERE?

In the early 1980s, when ARPANET was becoming the World Wide Web which grew into today's Internet, the focus was on interoperability and reliability as a means of communication and potential command and control in the event of an emergency. Everyone with access to the system knew each other and security was not a consideration. Then, in the late 1980s, trouble started; Robert Morris released the first worm (a self-replicating piece of malware) and Clifford Stoll discovered Soviet Bloc spies stealing U.S. secrets via a mainframe at the University of California, Berkeley. These were quickly followed by a number of incidents that highlighted the security risks associated with our new communication capability (see Appendix for list of major events through the years).

The key cyber events as they relate to and impacted the military occurred in the mid-to-late 1990s highlighted by Time magazine having a cover on "Cyber War." The 1998 Solar Sunrise incident hit the news as the Pentagon got hacked while America was at war with Iraq, but the instigators were actually just two kids from California. Then came Moonlight Maze, where the Department of Defense (DoD) found intrusions from systems in the Soviet Union (though the source of the attacks was never proven) and Russia denied any involvement (hackers will often route their attacks through countries that will not cooperate with an investigation so there was plausible deniability). By the early 2000s, a series of attacks, generally accepted as being from China, were identified and code named Titan Rain, the name was changed to Byzantine Hades after the Titan Rain code name was disclosed in the media and changed again when the Byzantine Hades code name was posted to WikiLeaks (current name is

http://dx.doi.org/10.1016/B978-0-12-416672-1.00002-7

classified). The term "Advance Persistent Threat (APT)" has become the common reference term for this state-sponsored systematic electronic reconnaissance/digital espionage. By late 2000s, there was a physical aspect added to the entropic attacks which the DoD code named Operation Buckshot Yankee. Thumb drives used by U.S. Military were found to have malcode embedded which caused DoD to ban thumb drive usage on all military networks and systems.

In addition to attacks on the U.S. Military, some international incidents occurred in the 2000s. In 2007, hackers believed to be linked to the Russian government brought down the Web sites of Estonia's parliament, banks, ministries, newspapers, and broadcasters. Estonia called on the NATO treaty for protection and troops to help recover. A year later cyber attackers hijacked government and commercial Web sites in Georgia during a military conflict with Russia, creating a new form of digital signal jamming over the Web. In 2010, the Stuxnet worm attacked the systems that control Iran's nuclear material development causing damage to these systems. While the examples we have looked at, a nation calling on a mutual defense treaty—combined kinetic/non-kinetic war and physical destruction of a national security asset, could be considered to be cyber wars no nation state has formally acknowledged or accused another state of "cyber war."

There are some notable commercial cyber events that parallel the military's pains. In 2009, reports revealed that hackers downloaded data from the DoD's multibillion-dollar F-35 Joint Strike Fighter program, showing that the cyber attackers were going after defense contractors as well as the military itself. Then in 2009, Operation Aurora broke into the news when Google publicly revealed itself as being one of many commercial companies hacked by the APT, showing that the cyber attackers were also going after commercial intellectual property. There were two more troubling attacks in 2011: The first was a series of hacks exposed in the global energy report "Night Dragon" which showed how China was trying to gain a competitive edge in the energy market through espionage. The second was the RSA attack where stolen information would allow a hacker to replicate the number that showed up on the password token many organizations used to secure their networks, showing that the enemy was willing to attack the infrastructure used to protect the U.S. More recently, a very detailed report on China's cyber operations was published by the commercial consulting vendor Mandiant. These all point to an active campaign to steal intellectual property. Some of the information is taken to gain military advantage but the majority is to gain an economic advantage which as we look at countries' ability to fund their militaries has a direct impact.

For the past 30 years, there has been a continuous battle between defenders and attackers on networks around the globe. At first most of the hackers were motivated by curiosity, looking for entertainment or bragging rights. Then as more financial transactions were conducted on the internet, a criminal element followed. Soon we saw trends like botnets where it did not matter to the attacker if the target was military, government, or commercial, the attacker was just after as many computer systems as they could acquire. This was back in the days when it was popular to say "network security needs to be good enough so that you're not the low hanging fruit on the internet." That is no longer true as with many sophisticated threat organizations there are a lot of giraffes on the internet interested in only eating fruit from the top of the tree; security today needs to be good—not better than the next guy. Then as nation's governments, militaries and economies became more dependent on the internet we see nation states acting against each other in cyberspace. As each new threat grows new protective solutions are established and new attacks are developed to circumvent them, and the cycle continues.

The threatscape map in Figure 2.1 was designed to assist everyone in understanding this complex environment. As we look at it some will see the map of Mordor from J.R. Tolkien's fictional Middle-Earth while others see the old TV show's map of the Ponderosa. The map is designed to show how all the events we have covered in this chapter interrelate in cyberspace. It shows the methodology (upper left) and resources (lower left) that hackers use to break into systems. Then it provides the different categories of the attackers in the second column. These categories are divided by a solid line but it is important to realize that nation states can use criminal organization to accomplish their aims or for another example where they can cross is between insider threat and hacktivists. In the past an insider might post an organizations' critical information on the internet, either because they were disgruntled or a whistle-blower, but now hacktivists are behaving like an insider threat by not stealing information but rather by posting it openly on the internet. The center column shows the defensive mountain range to portray the "defense in depth" strategy used to protect networks today. Finally, the far right column shows the different types of data the attacker wants access to. It is broken out by the motivations of the threat actors from the second column.

ATTACK METHODOLOGY WITH THE TOOLS AND TECHNIQUES USED TO EXECUTE THEM

As we examine the manner in which networks are broken into, it is evident that the basic steps in the process are analogous to traditional military attack/defend doctrine. Similar to how South Korea and North Korea have built physical defensive fortifications between each other, we see the same principle and even term used by network administrators—Demilitarized Zone (DMZ). This is where one puts systems that must connect to the internet where they are in more danger. From the attacker point of view the same steps are necessary to attack a network as it is to break through the DMZ: conduct reconnaissance to determine vulnerability, marshal forces at the point of weakness, attack and penetrate the defense, then exploit the infiltration to gain control over the battlefield/network.

The major difference between kinetic (real world) and non-kinetic (virtual world) warfare methodology is the weapons versus software programs they use. We will walk through the steps and define a few of the tools used. The tools will be covered in more detail in later chapters so this will just be to gain an initial understanding.

WARNING

The only difference between a hacker tool and a cybersecurity professional tool is "written permission." Please do not load a tool you read about here like the password cracker on an operational computer at work to test your organization's security without authorization. People have been fired for using these tools despite their good intentions. Contact your manager and get approval, in writing, then test your security in a coordinated and safe manner.

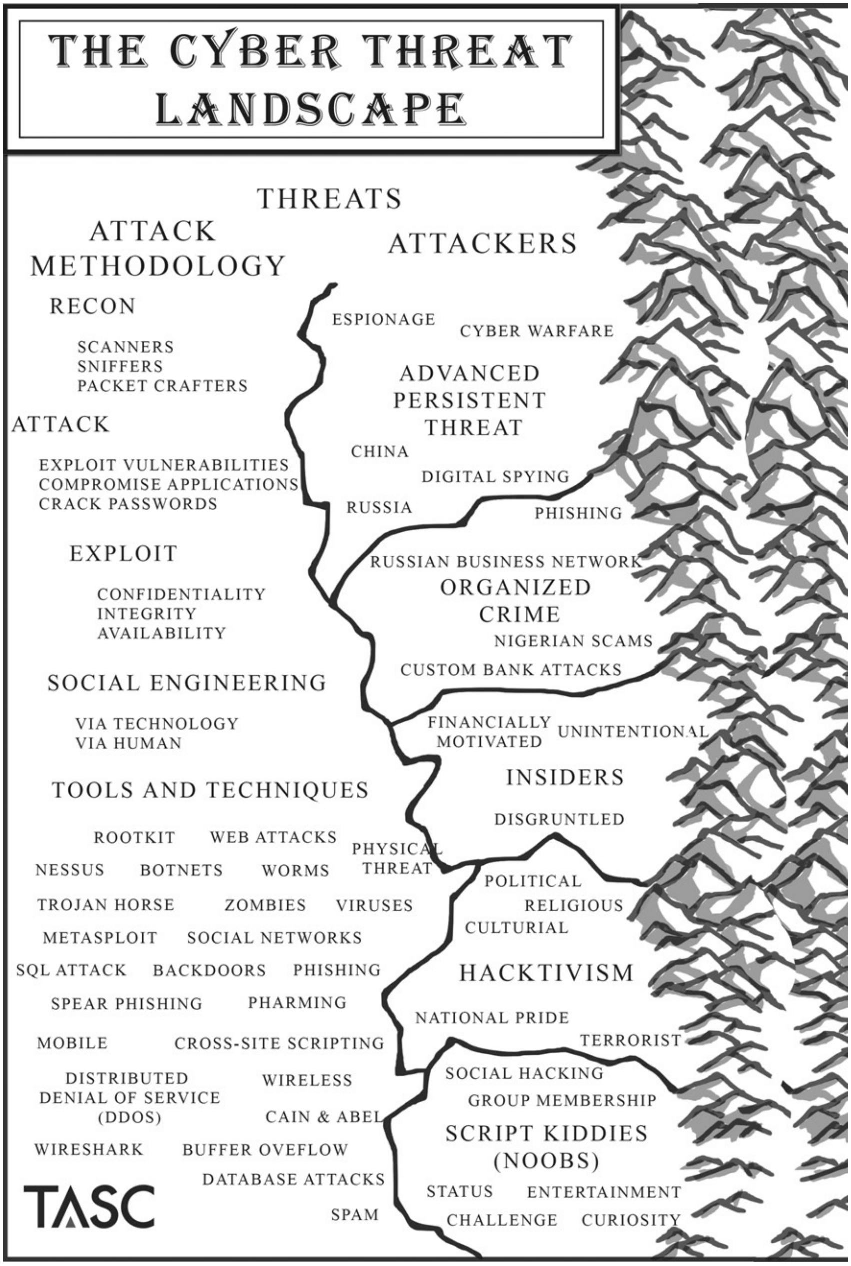

FIGURE 2.1 This is a threatscape map designed to show the different components in the cyber environment and how they interact.

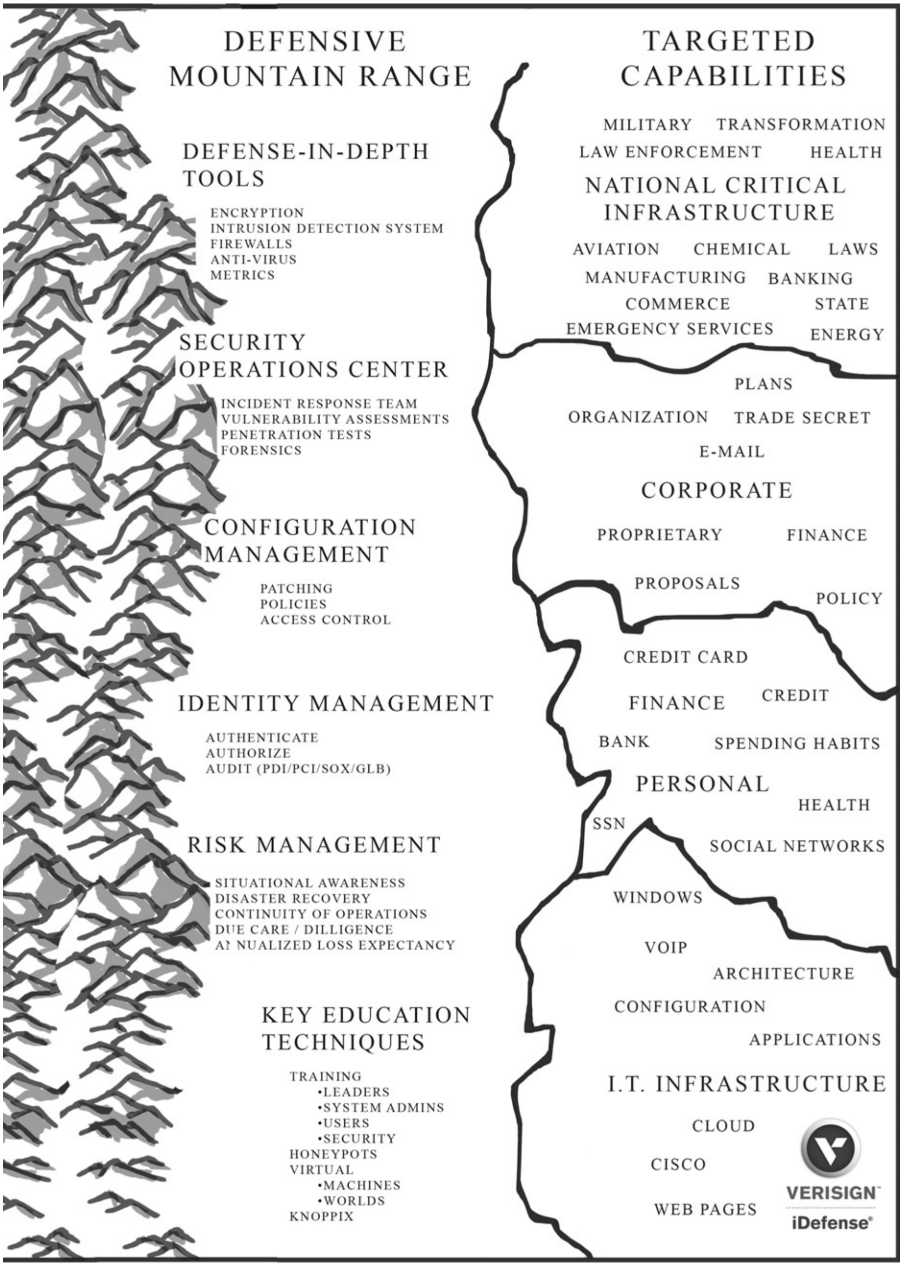

FIGURE 2.1—Cont'd

An attack methodology is the process or general steps used to conduct an attack of a target. The tools/techniques are what are used to execute the process. The major steps are recon, attack, and exploit. These steps can be a variety of activities, from launching machine to machine attacks to using social engineering. (Think of social engineering as scamming or conning a target out of information allowing the hacker to compromise a network.) Each of these steps or phases have a number of substeps to accomplish them and in many cases different hackers will both modify and automate them to suit their style.

Mapping Sample of Well-known Tools to the Process

- Reconnaissance
  - Scanners
    - Nmap
    - Nessus
  - Sniffers
    - Wiresharek
    - Ettercap
  - Packet Crafters
    - Netcat
    - Hping
- Attack
  - Exploit Vulnerabilities
    - Metasploit
    - Canvas
    - CoreImpact
    - Back Track
  - Compromise Applications
    - Web page—Cross-site Scripting
    - Database—SQL attack
  - Crack Passwords
    - Cain and Able
    - John the Ripper
- Exploit
  - Confidentiality
    - Steal data to use or expose
  - Integrity
    - Change data based on impact desired
  - Availability
    - DDOS based on critical timing
- SE
  - Via Technology
    - Social Engineering Toolkit
    - Maltego
  - Via Human or user
    - Phishing
    - Social Networking sites

To begin the recon phase a target is required. The target can be the specific systems that will be attacked or the personnel that use them. To attack the unique Internet Protocol (IP) address for a machine or Uniform Resource Locator for a Web page must be known. To conduct an attack via the users, a phone number could be all that is needed. IP addresses and phone numbers can be found with a quick Google search or with services like American Registry for Internet Numbers searches. Much of what is needed for a social engineering attack can be found on a business card.

Once the target is identified, the recon begins to find the weak point or vulnerability. The attack can be against the operating system or one of the applications on it (i.e., Adobe Flash, Microsoft Office, games, Web browsers, or an instant messenger). A scanner is run against the system to determine and list many of the vulnerabilities. Some of the more popular scanners are Nmap, Nessus, eEye Retina, and Saintscanner. Attack framework tools are available that both scan and then have the exploits to launch the attack matching vulnerabilities found built into the application. Some popular framework tools are Metasploit, Canvas, and Core Impact. Finally, there are tools that transform a machine into a Linux system by booting off of a Linux live CD. The most popular live CD attack tool is BackTrack.

Another tool that is useful during recon is a sniffer. This is a tool that has the attacker's system mimic every computer on the network so it gets a copy of all the traffic. It will allow the attacker to read all unencrypted emails and documents as well as see the Web pages being accessed by everyone on the network. Popular sniffers are Wireshark, Ettercap, and Tcpdump. On the wireless side tools include Aircrack-ng and Kismet.

While there are a lot of recon tools that are very powerful and easy to use, the one set of tools that shows how the threat environment has evolved is packet crafters. Someone with no programming skills can now craft unique attacks. Popular tools include NetCat and Hping. There are a host of other tools for recon but these represent the baseline tools used to discover the vulnerabilities that allow movement to the attack phase.

When attacking a system there are many types of malcode that can be used. At the code level there are worms or viruses that can use attack vectors like cross-site scripting or buffer overflows to install rootkits or a Trojan horse which acts as a backdoor into a system, and is used to spread the attack. A worm spreads without any help. It infects a system and then uses that system to find more systems to spread to. A virus needs some user interaction like opening any type of file (email, document, presentation) or starting a program (game, video, new app). Worms and viruses use techniques like cross-site scripting or buffer overflows which attack mistakes in the code in order to compromise it. Cross-site scripting is a Web-based attack that allows unauthorized code to be executed on the viewer's computer that could result in information being stolen or the system's identification certificates being stolen. An overly simplified example of a buffer overflow is when a program asks for a phone number rather than giving the 10 digits needed, the software sends 1000 digits followed by a command to install the malcode. Because the program does not have good error handling to deal with the large amount of unexpected extra data, it executes the malcode.

A rootkit is a program that takes over control of an operating system and tells lies about what is happening on the system. Once a rootkit is installed, it can hide the hacker's folders (i.e., hacker tools, illegal movies, stolen credit card numbers), misdirect applications (i.e., show the antivirus updating daily but do not allow it to update), or misrepresent the system status (i.e., leave port 666 open so the hacker can remotely access the system but show it as closed).

The first generation of rootkits was much like my daughter when she was 4 (called the fibbing 4s because that is when most kids learn to lie). Like a 4-year-old, the rootkits of the first generation did not lie very well. The generation we are on now is more like when she was 21 (she was MUCH better at telling a coherent story that was not easy to detect as a lie). The current generation of rootkits does a much better job of hiding themselves from detection. The next generation will be like someone with a masters in social engineering; almost undetectable. A Trojan horse backdoor is a program that masquerades as a legitimate file (often a system file: i.e., files ending in .sys on a Windows box or the system library on a Mac). These files are actually fakes and have replaced the actual system file. The new file both runs the system and opens a backdoor to the system allowing the hacker remote control of the system.

One use for worms and viruses is to build botnet armies. A bot (also called a zombie) is a computer that is a slave to a controller. Once someone builds an army of millions of bots they can cause a distributed denial of service (DDoS) by having all of the bots try to connect to the same site or system simultaneously. This can be done to blackmail a Website (pay or be blocked so no customers can get access), disrupt command and control systems, click fraud (if Acme.org gets paid one cent for every customer that clicks on link taking them to Selling.com a botnet could be used to do that millions of times a day) or compile complex problems (much like a distributed supercomputer).

NOTE

If the intent of an attack is to cause a Denial of Service (DoS) there are two ways to accomplish this. The first is to attack the system and take it down. The second (usually called Distributed DoS or DDoS) attacks the bandwidth. In cases where you are attacking the communication lines you can skip recon because you are not worried about finding a specific vulnerability, you just need a botnet army large enough to overwhelm a target's communication capabilities. If you are attacking an organization with distributed and redundant infrastructure then it would be necessary to develop malcode that attacks the organization's systems simultaneously to take it offline as it is impractical to take down all the communication capabilities.

There are a number of ways to launch attacks targeted at a specific system rather than the broad net a worm or virus would catch. The attack framework tools mentioned earlier are the most common. The key is to correlate the exploit to the vulnerability. Much like there has never been a bank built that cannot be robbed and there is not a computer or network that cannot be broken into given enough resources and persistence. If no vulnerability can be found then the attacker can go after the authentication via password attacks, credential compromises or attack the security infrastructure used to protect the network.

Cracking passwords can be done with brute force by having a program try every possible password iteration. This can be time consuming and is easy to detect but, depending on the strength of the password, is very effective. If the hacker can get access to the password file then tools like Cain & Able or Jack the Ripper can be utilized to crack them. Another technique that is available is called rainbow tables. These are databases where popular password encryption protocols have been run on every possible key combination on a standard keyboard. This precompiled list allows a simple lookup when the hacker gets access to the list of encrypted passwords. Many of these tables have done every combination for 8-20 characters and the length grows as hackers continue to use botnet to build the tables.

NOTE

Exploit has three meanings within the cyber community. When talking about code it refers to malcode that allows a system to be compromised. When talking about attack methodology it refers to what the payload of the attack is intended to accomplish. When talking about military doctrine it is used by the intelligence community to refer to cyber recon/espionage.

The exploit phase is where the attacker takes advantage of gaining control. There are generally three factors that the hacker can compromise: Confidentiality, Integrity, or Availability. When attacking confidentiality they are simply stealing secrets. Integrity attacks are when they change the data on the system or masquerade as a legitimate authorized or authenticated user. In a commercial setting this could be changing prices or customer data. On a military network it might be to change the equations used to calculate command and control guidance. Availability attacks are normally time based and can be accomplished by taking the system down or overwhelming the bandwidth. The type of exploit is based on the motivations of the attacker. They can use the system to attack more systems on the network, misrepresent the user (send fake emails), or load a rootkit with a backdoor to maintain long-term access. They will often try to avoid detection and might even use anti-forensic techniques like log wiping and time stomping. Some will patch the systems they have taken over so future hackers will not be able to break in and take them away. Finally, they may load digital tripwire alarms to tell them if they have been detected by security engineers using forensic tools.

If these technical attacks do not work another vector of attack is social engineering. In fact some threat organizations use social engineering as their primary means of attack. Social Engineering (SE) can be thought of as the act of influencing someone's behavior through manipulating their emotions, or gaining and betraying their trust to gain access to their system. The difference between social engineering and other attacks is the vectors are through the person, or as hackers say the "wetware." Think of any of the movies about stories or movies about con-artists, the difference being rather than money they want access to information on or about a target's computer systems. This can be done in person but is often done over the phone or remote communications like email. It starts with pre-texting, with includes researching an organization using sources like websites, social media, or even meeting people at places like a conference to exchange business cards. The most common attack today is via email. This kind of social engineering attack is called phishing (sending general email to multiple people), spear phishing (targeted at a specific person), or whaling (targeting a specific senior member of the organization). There are also technical tools like the "Social Engineer Toolkit" that are designed to assist attacking the workforce.

ATTACKERS (MAJOR CATEGORIES OF THREATS)

This section will focus on the different categories of attackers. As we look at the threatscape map (Figure 2.1) the attackers are not ranked or ordered in any particular way. Again it is important to note that while there are solid lines between them they can overlap or someone can belong to more than one category. The Advanced Persistent Threat (APT) can buy exploits from criminal elements, noobs can join hacktivist causes and, one particularly troubling paradigm shift that has happened recently, hacktivists can behave like insider threats as they steal information and then publish the stolen information on the websites like WikiLeaks.

Advanced Persistent Threat

APT is one of the key drivers of cyber warfare. The term APT is often used in different ways by the media, but, for purposes of this book, APT means state guided attacks. It is truly digital spying or espionage in the virtual world. Some of the most commonly referenced APT activities were discussed earlier (Titan Rain, Operation Buckshot Yankee, Aurora, Stuxnet, Night Dragon, APT1 Report). As we examine if the APT actions qualify as war we look to how war is defined.

Organized Crime

Organized crime on the Internet is widely covered in the news today. One of the most often joked about scams on the Internet is the “Nigerian royalty that just needs access to your bank account to get money out of the country” scam that sends phishing emails designed to steal identities and access the victims’ bank accounts. The text of the emails from the Nigerian scams will talk about how they have money that they need to get out of the country and all they need is to transfer the money to a U.S. bank, but to do that they need access to the victim’s account. The early versions used poor English but they have gotten much more sophisticated over time. These scams have been around long before the Internet but have become much easier to do in bulk and with little risk of incarceration, as the perpetrators are usually overseas. Another popular scam is selling fake medicine. While some of the sites are selling legitimate drugs most will send fake medicine if they send anything at all. Similar scams can be used to get members of the military or national security infrastructure to get involved in activities they would not do in the real world.

One of the more well-known criminal organizations is called the Russian Business Network (RBN) also known as the Russian Mob (note this is not one single organization). If someone graduates from a university in one of the old Soviet Union bloc countries with a degree in computer science one of the better paying jobs is with the RBN. There they will work full time on tasks like building custom exploits targeting specific financial institutions, building botnet armies, running identity theft networks, or any one of a dozen of “business ventures” for organizations like the RBN based on different revenue models. These organizations can be staffed in one country, use systems hosted in a different country (for a while RBN was using systems hosted in China) and commit crimes against citizens in a third country. This makes it very complex to prosecute when the crimes are discovered. A great reference that goes into detail is the book “Fatal System Error” by Joseph Menn. While we have talked about China and Russia they are not the only countries that have cyber-based criminal organizations; in fact the U.S. has similar groups.

Insider Threat

As we change to look at insider threat you will find a common rule of thumb is that insider threats represent 20% of the threat but could cause 80% of the damage (recent studies by CIS and Verizon show the real numbers of insiders are closer to 50%). The reason is the insiders understand what is valuable on the network and often have legitimate access to it. The three basic categories of insiders are: disgruntled employees, financially motivated (thieves), and users unintentionally causing damage. Disgruntled employees can cause problems by publishing information on the Web to competitors or to fellow employees (i.e., everyone's salary). They could also install a logic bomb that will cause damage if they stop working at the company (i.e., if Winterfeld does not show up on the employee payroll, reformat all servers in the data room). Financially motivated insiders will misuse the company assets or manipulate the system to steal. There are both intentional and unintentional insider threats. Examples of unwitting threats include users who unintentionally delete files causing loss of work or accidentally post classified documents on unclassified systems causing what is known as a spill. Spills could require destruction of the system and a lengthy investigation. Finally, users can open files or go to websites with malcode infecting the network.

Hacktivist

Hacktivists can be motivated by political views, cultural/religious beliefs, national pride, or terrorist ideology. The most notable example has been from a group called Anonymous. This group of loosely affiliated hackers from around the world banded together to attack organizations they felt were in the wrong. This cyber vigilante group attacked the Church of Scientology under project name Chanology in 2008 and started using their trademark saying "We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us" [1]. They have attacked MasterCard for stopping support of WikiLeaks, Law Enforcement Agencies for policy they do not support, political parties, HBGary Federal (in response to statement made by Aaron Barr), Sony (in response to a lawsuit they brought), the Bay Area Rapid Transit system (in response to their closing down cell phone tower coverage at the stations to prevent a protest), porn sites, and many government sites around the world. Their supporters can often be seen wearing Guy Fawkes masks from the movie "V for Vendetta." As of early 2013, the FBI has arrested many of the leaders of Anonymous, but the group is still active and expect more groups like this to sprout up. A good reference to read on the story is "We Are Anonymous: Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency" by Parmy Olson.

Script Kiddies/Noobs

The final group in this section is on Script kiddies or noobs (for new to hacker). These are pejorative terms for the less skilled hackers. These are the people who just use the tools that can be found on the Internet with little thought out methodology or technique. They have many different motivations to start hacking. Some are looking for a social experience and will try to join a hacker group (some groups will require proof of hacking ability before they grant membership), others enjoy the challenge or want to gain status across the hacker community, still others do it out of curiosity and think of it as entertainment. We can see many examples of these at hacker conferences like DEFCON, ShmooCon, or HOPE. The problem these script kiddies pose to the cyber warfare landscape is the amount of activity they produce. If there are millions of attacks launched by noobs every week, how can the APT or specific criminal activity be located? It is also important to understand that the tools script-kiddies use are very powerful and they will end up PWNing (slang for own) systems. The age old adage "the defender has to get it right every time while the attacker only has to get it right once" applies here. The Defense Information Systems Agency has consistently said the majority of systems compromised were from known exploits that could have been prevented if the systems were fully patched and configured to standard [2]. As script-kiddies gain more experience they will become hackers and usually end up being part of some group.

These groups are not represented in the threat list as they do not fit into an attacker category. When they join together they may prank each other, build tools (one classic example is the Cult of the Dead Cow's tool called "Back Orifice" in 1980), they may live near each other (i.e., 303 group in Denver), skill focused (Social-http://www.social-engineer.org/ group), startup conferences (B-Sides) or run a podcast (pauldotcom). This would be an example of the range of motivations—some are white hat and only use their skills when professionally contracted to test security, others are gray hat and do what they feel is the right thing for betterment of the Cybersecurity community and some are black hats who conduct illegal activities.

DEFENSE IN DEPTH—HOW ORGANIZATIONS DEFEND TODAY (DEFENSIVE MOUNTAIN RANGE)

On the threatscape map (center column of Figure 2.1) the Defensive Mountain Range shows many of the different methods used to protect networks today. It covers the infrastructure and processes used to secure the systems and detect any intrusions. Much like real-world defenses, they need to be constantly validated, monitored, and updated.

Defense-In-Depth or multiple layers of protection is how most networks are protected today. The issue is there are so many mobile systems (laptops, phones, tablets) and removable storage devices that it is becoming increasing difficult to keep all the systems inside the defensive perimeter. Some of the critical tools are firewalls to block the attacks, intrusion detection systems to alert on attacks, antivirus to kill the attacks that got through, and encryption of the data on the device so if the device is lost or stolen the information is still secure. The critical process needed is good security metrics. Metrics revolve around the need to quantify the impact of cyber events. They should support both the technical and senior leadership's ability to make decisions to protect the network and react to changes in risk assessment as well as support understanding of return on investment of security infrastructure. There has been a lot of work done, but there is no clear set of industry standard cyber metrics today. There are three basic types of metrics:

- *Technical:* Based on infrastructure and the incident response cycle.
- *Security return on investment:* Cost-based analysis on benefits from implementing new technology or policies. These goals must be set before they change and methods to track performance are established.
- *Risk posture:* Analysis on impact of cyber events/incidents to enterprise and operations.

Next comes the team that monitors the network, usually called the Security Operations Centers (SOC) or Computer Emergency Response Team. These cells typically contain the Incident Response Teams responsible for the response cycle—Protect, Detect, React, and Recover. This is very similar to the military OODA Loop (Observe, Orient, Decide, and Act). The SOC would also be responsible for conducting Vulnerability Assessments (VA) and Penetration Tests (PT). The VA is designed to look for vulnerabilities on the network then prioritize how to fix or mitigate them. The PT is designed to test the team's ability to respond to an intrusion. Penetration Tests can also be called Red Teaming depending on the scope and interaction of the two sides. The PT team will not only find the vulnerability but exploit it and once they break in will either grab a predetermined file (called the flag) or load a file on the system (called the golden nugget). Then the SOC team must determine how the PT broke in and what they did. This will validate the team's processes and tools. One key capability that is needed after an intrusion is the forensics expert. This is someone that understands the rules of evidence and can testify in court. This analysis is key to understand what happened to prevent it from reoccurring.

TIP

A forensics expert is a must-have team member, but, as they can be expensive, many organizations have someone they can call on demand as opposed to having a full time staff member. The forensics expert should be called if there is any possibility of a lawsuit, human resource action (firing), or prosecution of the hacker. There must be clear policies on when they are called because, much like a real crime scene, the more people that have accessed the data the more the crime scene is compromised. The military is slowly moving toward gathering evidence in a way that it can be presented in court as opposed to just getting the systems back on line quickly.

Configuration Management is a critical part of the defense. A well-configured and managed network is more secure. Think of walking up to a cruise liner to start your vacation only to find it is so covered in rust you cannot tell what color it used to be painted. Common sense would prevent you from getting on. Yet because we cannot see that our network devices are past their maintenance lifecycle we put our most valuable information on the equivalent servers. The basics require timely patching. Patches must be tested before they get installed on critical operational systems so the challenge is how much time is allowed for analysis (some suggest 72 h, but that can be expensive so there is a broad range). Well understood and enforced policies for both the users and network administrators are a must. They both can impact the security baseline with decisions on operations or processes but often do not examine the impact to security risks. Finally, access control must be managed so that only the people with a need are allowed to access the mission critical data. This can be done physically or through electronic policies. This is called the principle of least privilege and has been used for decades in the intelligence community.

Identity Management is one area that will help as users become more mobile. The three vital factors are authentication, authorization, and audit/compliance. Before someone logs into the system they should have to prove who they are with something they know (user name and password), something they have (electronic token), and/or something they are (biometrics, i.e., scan a fingerprint): this is authentication. Next they should be categorized by what kind of information they should have access to. The military uses Unclassified/Secret/Top Secret but there are a number of organizations that have designed their own system. Finally, as was mentioned earlier, as every network will have a weakness over time it is prudent to assume that someone has penetrated the network and conduct audits to find them.

Compliance is based on the legal or regulatory requirements of the industry. Some examples are:

- Healthcare = Health Insurance Portability and Accountability Act (HIPAA)
- Finance = Gramm-Leach-Bliley Act
- Publicly traded companies = Sarbanes-Oxley Act
- Credit Cards = Payment Card Industry
- Energy Providers = North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) program
- Federal agencies = Federal Information Security Management Act (FISMA)
- U.S. Intelligence Community (IC) = Director of Central Intelligence Directive (DCID) 6/3
- DoD = DoD Information Assurance Certification and Accreditation Process (DIACAP)

Today most of these are based on annual reviews of the systems but they are moving to real-time monitoring.

Risk Management is what all these regulations have been driving to. The goal is to achieve Situational Awareness (SA). SA is the correlation and fusion of data from multiple sources that enable decision making. Ideally it will be presented visually through a Common Operational Picture that will facilitate true risk posture understanding and provide information in a format that enables decisions. If the network is lost then the Disaster Recovery (DR) and Continuity of Operations Plans (COOP) come into play. DR focuses on getting the network back up while the COOP is the plan to continue operations without any automation.

As we design systems and networks it is important to understand there are legal expectations of how the network will be protected. These principles are known as due care and due diligence. These should be based on the "Annualized Loss Expectancy" calculations (Vulnerability × Threat × Asset Value = Total Risk then Total Risk × Countermeasures = Residual Risk). This will help determine where the organization is in the security lifecycle: requirements definition, design and develop the protective measures, implement, and validate the defensive solution, operation maintain risk management controls. This will also allow security to be designed into the system rather that bolted on afterwards, something that is always more expensive and less effective.

One of the most effective protection techniques is education designed to alter the users' behaviors. The training must be targeted at the different types of users: leaders need to know how to manage cyber risk, system admins must understand the importance of configuration management and patching, general users need to understand how their behaviors can become vulnerabilities that hackers can exploit, and the cyber security team needs to understand the latest threats and protection tools/techniques. Some useful tools are honeypots, virtual machines, virtual worlds, and live CDs. Honeypots are systems that are deployed with no operational function so any interaction with them causes an investigation. If we install a server with data labeled "senior leaders evaluations and important financial data" it will attract insiders and hackers but as soon as they touch it the SOC will be alerted and quickly react. Virtual Machines (VM) are software-based computers that allow anyone to simulate multiple computers with various operating systems on their computer. This allows them to test hacking from one VM to another. Virtual worlds can be used to conduct training with no travel costs. A popular business-oriented virtual world is Second Life. Finally to boot your current computer as a Linux machine to use some of the tools we have discussed, use a live CD like BackTrack.

WHAT THE THREAT IS AFTER (WHAT WE SHOULD FOCUS ON DEFENDING)

Targeted Capabilities break out the variety of systems, types of information and industries that the enemy is trying to compromise. The major categories are National Critical Infrastructure, Corporate, Personal, and Information Technology (IT) Infrastructure. Critical infrastructure often has aspects of the other categories embedded within it. Corporate information will normally have personal and IT Infrastructure embedded.

National CIP includes: Banking, Law Enforcement, Laws/Legal System, Transportation, Health, Military, Chemical, Energy, State, Emergency Services, Plans, Manufacturing, Commerce, and Aviation. If any of these were not available for even short periods of time, there would be major impacts. The loss of faith in the security of aviation after the 9/11 attacks had secondary economic impacts. The loss of belief in the integrity of our financial systems could cause a run on the banks. If the power grid were to be taken down it would cause both economic and health impacts. The issue is that most of this critical infrastructure is managed by commercial companies that have to balance risk against profit and are generally driven by cost-effectiveness, functionality, and financial gain, rather than security.

Corporate assets such as email accounts, proprietary info/trade secrets, finance records, policy, proposals, and organizational decisions are all of value to the competition. Depending on the nature of the information nation states, criminal organizations, hacktivists, and insiders could all be after different parts of the company.

Personal data like health records and financial information (banking and credit card accounts) are high value targets for insurance companies, criminals, espionage targets, and your personal enemies. If someone wants to target a senior member of the U.S. Military today, finding out as much about the person on the Internet would be the first step. The same could be true of Law Enforcement Agencies that focus on the drug trade. Digital natives are putting more and more personal information on the Web. This information all ties back to two major issues: identity theft and social engineering.

IT infrastructure is a target for two reasons. Hackers may want to use the infrastructure for themselves (i.e., building a botnet) or they want to know what operating systems (i.e., Windows/OS X) and network devices (i.e., VoIP, applications, and specific Cisco devices) are available to allow them to find vulnerabilities. Understanding the architecture or mapping the Web pages could provide insight into how to gain unauthorized access.

SUMMARY

This has been an overview of the threatscape coving the methodology, tools, and techniques used by the different types of attackers and a review of the key parts of the defensive infrastructure employed to protect our systems as well as the general categories of information the attackers are after. These will all be covered in more detail in subsequent chapters but this foundation is intended to help tie it all together. Chapter 15 on Cyberspace Challenges is designed to give an overview of the cyber environment, focused on the challenges. It breaks out the problems in a way that they can be evaluated against each other and facilitates a discussion on prioritization and resource allocation.

The question most often asked after discussing this cyber threatscape is how someone should protect themselves at home. The answer is "safe behaviors!" The basics go a long way such as a firewall, up-to-date antivirus, patching all applications, keeping private and financial data on a removable hard drive that is only connected when in use, and BACK UP valuable data to a place that will not be destroyed if the system is stolen or destroyed. All are mandatory for basic security, but they can all be defeated by poor security practices such as weak passwords, surfing sites known to be hot spots for malcode, and opening emails or accepting invites on social networking sites from someone unknown. While there is no such thing as "security through obscurity" we should strive to not be the "low hanging fruit" that is easily PWNed.

References

[1] Anonymous. UNK [Online], http://www.webutation.net/go/review/anonymousarmy.webs.com.

[2] Brig, Gen. Patterson, LaWarren. Brief on operating, maintaining and defending the Army's global network enterprise. In: Cyberspace symposium, Colorado Springs; 2010.