Global Information Assurance Certification Paper

Curious to Criminal: Sophisticated White Collar Crime of the Future

George Meier

GSEC Practical (v. 1.4b) option 1

Abstract

As laws combined with increased security measures discourage curious juveniles and simple thieves, white-collar crime of the future will become more sophisticated, more costly, and less detectable. This document presents a brief assessment of today's common threat agents along with a description of the threats they pose. The threat agent of the future is described and the assets that a future threat agent might target are presented. Finally, possible threats to those assets and safeguards that can be put in place to thwart and detect the threats are explored.

Introduction

As individuals, companies and governments have come to rely on computers as a cornerstone of their critical infrastructure, the significance of threats to confidentiality, integrity, and availability have increased. The utility of computers has increased as computers have become more interconnected. However, increased accessibility has also allowed a greater exposure to the purveyors of threat, which in this paper will be referred to as threat agents. An early example of one such threat caused by the networking of computers was the Morris Worm (Kehoe). In 1988, the Morris worm quickly spread around the early Internet resulting in many computers becoming unresponsive. Even in the early stages of the Internet, while still in an academic setting, the potential threat to availability was apparent. Now, many years later the Internet is deeply embedded in our society, and using the Internet is as common as utilities such as electricity and telephone. In business, the Internet has become a common, if not necessary, part of the supply chain. This reliance is because the Internet is commonly used to connect customers to businesses and businesses to their suppliers. As a result of this reliance on computer systems, security has become even more challenging. For example, costly, even if sometimes unintentional, threats to availability from autonomous programs, include the "I Love You" virus which crippled E-mail servers, Nimda and Code Red which spread virulently on IIS servers, and recently networks were debilitated by UDP packet floods from the SQL Slammer worm. These programs threaten computer systems by exploiting security weaknesses. A method is to take advantage of poor application security designs that can be easily tricked into executing foreign scripts or binary code. Another method is to attack poor implementation, such as not validating the amount of input, which may result in a buffer overflow. A buffer overflow is another method to cause foreign binary code to be executed. In contrast to these programs, non-autonomous, very intentional threats to availability have occurred via distributed denial of service attacks, such as those to the Domain Name System root servers. However, the majority of successful

automated and distributed attacks to date, while costly to the effected targets, and have largely been threats that did not result in a monetary gain for the threat agent.

Attack Methods

Attacks effecting selected targets have also occurred. These attacks have involved complex techniques that target implementation deficiencies of protocols and applications. While these smaller scale threats may not be nearly as pervasive, they may be an effective way for a threat agent to access valuable information. Many of these are more difficult to perform if the threat must pass through routers or firewalls. However, an employee or program on an internal local area network may be able to use these threats more successfully.

Threats to State Information. State information is like a bookmark that allows a program to determine which operations have been performed. State information is used to make discontinuous multiplexed data streams appear as continuous data streams. Threats to state attempt to cause one of the multiplexed information streams to be accessed by the threat agent. State in an HTTP session is kept using Cookies. Cookies can be stolen or forged by correctly predicting the cookie, intercepted by a man-in-the-middle, or read from a hard drive. The stolen Cookie can then be used to impersonate a user. This might allow the threat agent access to online banking or other financial transactions such as an online stock trade. Firewalls that do not track the state of a TCP connection can also be tricked into letting data through. TCP connections use a three-way handshake to establish the connection. The first part of the three-way handshake is a packet with the Synchronize bit is sent, and then the second part is a reply to that packet with the Synchronize, and Acknowledgement bits set. Firewalls that do not keep track of state assume that if a packet is seen with both Synchronize and Acknowledgement set, that the firewall should let the packet through because the packet should be a reply. Another kind of threat to state is connection hijacking. Packets are sent with sequence numbers. A spoofed packet with valid sequence numbers could be received from a threat agent before the authentic sender. As a result the authentic sender's packets are no longer in sequence and are ignored by the receiver. The threat agent then continues impersonate the authentic sender.

Threats to Cached Information. Caches store a temporary copy of data so that data can be accessed more quickly. The Domain Name System attempts to cache queries that convert the host name to an IP address. This is done so that a query to an authoritative source is not needed every time a request is made. DNS cache poisoning attempts to send false updates to a DNS server attempting to cache the query. When the poisoned entry is resolved the attackers IP address will be returned instead of the correct address. For instance, a user would see the correct URL displayed in their browser window, but because the cache was poisoned a threat agents site designed to gain the user's confidence

is displayed. In this way, a threat agent can steal confidential information by appearing as a trusted site. Another example is when authentication is based only on the username and fully qualified domain name from which a connection originates, such as the rhosts file.

Threats from Unvalidated Input. Threats from unvalidated input occur when the threat agent sends a specially crafted message, causing the server to act in an unintended way. Examples of this include SQL insertion attacks, whereby additional SQL commands are sent, which result in confidential information being accessed or modified (Anley). Another form of this threat, Cross Site Scripting, attempts to trick web site visitors by inserting HTML tags, which can display an untrusted site in a frame so that the untrusted site appears to be part of a trusted site. Another result of unvalidated input is a buffer overflow. A buffer overflow can result from not checking the size of the input data compared to the amount of memory allocated to hold that data. If the input data is able to over write the execution pointer, then some part of the input data could be executed (Chien). The result is foreign binary code executing with the permissions of the program that requested the input.

Packet Modification. This may include spoofing an address to hide the source, or deceive the receiver to believe that the packet is from a trusted source. A false source address might be used in forged UDP packets sent to a Syslog server to falsify log entries (bELFaghor). A false source address might also be used to pass through a firewall that filters on IP address alone without regard to the interface that the packet traverses. Fragmented packets could be used to evade detection by Network intrusion detection systems that examine each packet without regard to the others. The threat agent could carefully divided the attack among the fragments to avoid detection.

Replay Attacks. A replay attack occurs when some piece of information can be captured and replayed at a different time. For instance, some protocols authenticate by sending a token rather than the user name and password. While the token may expire at some point an threat agent who records and reuses the token before the expiration time may be able to gain whichever access privileges the token conveys. Smbproxy is an example of program that can record an NTLM hash, and replay it (SMB).

Brute Force Attacks and Dictionary Attacks. Brute force attacks attempt to try every combination of letters, numbers, and symbols until access is granted. Dictionary attacks try every word or common permutation. This is effective because many people choose passwords or pass phrases composed of words, or simple permutations of words.

Misconfiguration. When services or permissions have been configured correctly, a threat agent or curious user may access or modify data that they should not be able to. Sporadic revalidation of system configuration and permissions can

ensure that no purposeful or accidental changes have taken place that may threaten security (Boulanger).

Defining a Script Kiddie

Script kiddies are often young men seeking recognition from their peers. Often they have little knowledge about how to compromise a system, and may not even possess the skill to modify a variable in a shell script (Gordon, "Technologically"). These skills are not necessary because prepackaged tools and tutorials can be gathered from the Internet. These individuals often spend so much time interacting with the computer that they do no realize how their actions affect human beings. They would likely be adolescents who can be classified in the second stage of Kohlberg's model describing the development of ethical behavior (Gordon, "Generic"). Individuals in this developmental stage believe that every individual is responsible for what befalls them (Gordon, "Generic"). As a result of this perception, they use tools and follow instructions without feeling ethically responsible for their actions. As these individuals get older and progress through the stages of Kohlberg's model, negative pressure from a valued peer group, will cause them to give up the unpopular behavior. (Gordon, "Generic") Of concern are those individuals motivated by revenge or greed or who have no influence from a peer group that regards their behavior as negative. If normative influences are not effective, the behavior will continue.

Who Discovers This Information

Information used as a threat to computer security originates from a variety of places. In some instances, it is a creative use of a feature built into the software, such as null sessions (Details). Other times it may originate from the discovery of a programming mistake, such as a buffer overflow. Once security researchers identify a vulnerability, then they must decide who to tell and when to tell them. Although a few formalized recommendations have been drafted or proposed, none have been universally accepted. However, the person or group responsible for the discovery often notifies the vendor of the product, in order that the problem may be remedied and a software update be made available. Depending on the severity and exploitability of the problem, a vague description of the problem may then be released. This release allows system administrators to take appropriate measures to prevent the vulnerability from affecting the systems for which they are administratively responsible. Code that can exploit the vulnerability may also be released, both to encourage the vendor to fix the problem quickly, while simultaneously providing a practical method for system vulnerability testing.

The Social Effects of Law

Law influences accepted social ethics by affecting the pool of people who hold a minority point of view. The minority's ability to communicate can be

eliminated as a result of isolating members of the minority from each other. Increased isolation can be caused by the application of the penalty stage of a law, such as incarceration, or probation, such as forbidding access or distribution of information. Fear of the penalty may cause those who knowingly break the law to hide their activities, thus making it harder for new people to learn and adopt the minority point of view. Reduction of communication among a group that relies on computers to communicate may also result in an increased interaction with the majority, who may have been excluded from the minority's virtual computer world. In addition to those two possibilities, reduction of communication has a two-fold impact. First, it changes the proportional size of the majority, and then it eliminates the non-linear psychological advantage of having at least one ally, which can be critical in small groups. This results in a reduction of the minority's ability to resist normative pressures (Brehm 485).

Prosecution Versus Persecution

Because legal, economic, and social incentives may increase the prosecution of computer related crimes, individuals have further incentive to hide their activities. While obeying the law is important, it is equally vital to ensure that prosecution of computer related crimes does not develop into a type of witch-hunt. Prosecution has become a frightening reality for individuals who disclose computer security related information without malicious intent. Some aspects of laws, which border on persecution, have been exhibited. The arrest of encryption researcher Dmitry Sklyarov, threats from HP toward security researchers, silencing Professor Edward Felton about the findings of his research, and the arrest of the author of the T0rn Root Kit are all examples of this frightening legal trend ("FBI"; Bowman; McCallaugh; Oppenheim; Poulson,). Laws are starting to gray the line between creation and criminal application. Language in the Computer Misuse Act (United Kingdom) implies that, "it does not have to be proved that the defendant had any specific computer or data as [a] target in mind" (Sieber). Security researchers need access to discover and develop tools and techniques to adequately test their defenses against known threats. Thus it is important to eliminate the script kiddy's subculture, while retaining the technical information important to verifying and researching information security. While laws such as the Computer Fraud and Abuse Act (United States, 18 U.S.C.), the Digital Millennium Copyright Act ("Digital") and the UK's Computer Misuse Act (United Kingdom) may have the desired effect of a reduction in crime and changes in social ethics, these laws have also hindered the verification and research of information security issues.

Law and Business

Laws such as the Health Insurance Portability and Accountability Act ("Health"), the Graham Leach Bliley Act ("Gramm") and some of the financial provisions of the USA PATRIOT Act ("USA") have had a positive impact. These laws have caused financial services and health care providers, their vendors, and

the Vendor's vendors ad nauseum to improve their security measures, in order to be compliant with these laws. This trickle down effect has resulted in increased security not only for such businesses as banks and hospitals, but also for all the additional markets in which their vendors participate. Of course, the United States is not alone; the European Union has passed laws (Council, Additional; Council, Convention) with regard to the security of personal information and recommended the implementation of standards such as ISO 17799 (European). Through the proper implementation of these laws and recommendations businesses will be more able to avoid compromise by simple viruses and script kiddies, and better able to detect and prevent more complex threats.

The Impact of Law on Future Crime

Society will be affected as businesses do not feel economically threatened by reporting computer crimes and the number of successfully prosecuted computer related crimes increase (United States, VNU). Higher prosecution rates will be made possible as businesses increase their awareness of security issues, and implement comprehensive practices and procedures. The retention of detailed logs of high integrity combined with effective auditing and incident response will aid in the prosecution of computer-related crimes. The combination of these factors will in turn discourage and significantly reduce the number and effectiveness of casual threat agents. However, as the European Union has noted, "what began as a nuisance activity (often described as 'hacking') has highlighted the vulnerabilities of information networks and motivated those with criminal or malicious intent to exploit these weaknesses" (European). Thus, as observed by recent press releases from the US Department of Justice (United States, Computer), criminals have started to use computers for crimes in which computers are used as the means to a criminal end. These individuals do not commit crimes as a method to obtain peer recognition (Gordon, "Generic"), however, the contrary may be true, as they attempt to be undetectable. Often, the criminal's goal is financial gain, although, it is possible to envision scenarios in which computers are used for sabotage or to spread misinformation.

From Whence the Significant Future Threats Originate

Threats are often envisioned to originate from outside a business, where the threat might masquerade as a customer or supplier. This assumption results in very strong perimeter defenses. A single strong outer defensive layer provides a false sense of security. Multiple layers of defense are important in the event of breached perimeter defenses and also because the most significant threats may come from within. "On a per-company basis, one in every 23.7 employees was apprehended for theft from their employer" (Loss). Thus, in a company of one hundred people, only four of the employees who attempted or committed theft will be caught. Employees most likely to commit theft or fraud will likely have several traits in common. They will likely be male and exhibit some of the following traits: an external locus of control, strong competitive drive, preference

for risk-seeking, impulsivity, ability to rationalize behavior, unconformity or rejection of social mores, fear of failure, or low self-esteem (Krause). Additional identifying factors may include: alcohol or drug addiction, mental illness, criminal history, and financial problems (Krause). Work environment characteristics that promote theft or fraud include: easy access to assets or poor security, ineffective supervision, strong pressures for profit or gain, weak professional ethics or corporate values, lax prosecutorial approaches, lack of job satisfaction, low employee loyalty, pay inequity, anger or alienation or revenge, and greed (Krause).

Information Threat Agents Seek

Many computer users do not realize the amount of valuable information that computers contain that a thief may be interested in harvesting. Theft is not limited to traditional financial crimes like embezzlement or stealing inventory. Many computers modify and access information that may be of value to thieves. Banks and other businesses that process financial information are obvious targets. It is not rare for employees or contractors of banks to try to steal funds. Although the Equity Funding scandal happened in the early 1970's, it is a good example of how computers can be used to create false assets. In the Equity Funding scandal, software was created for the express purpose of manufacturing fraudulent policies (Mannes). Another example of fraud could be fraudulently modifying a customer's order to meet sales quotas, or adjusting inventory records so that stolen inventory will not be noticed. Trade secrets and intellectual property, like customer databases, present a target that may be of value to competitors. Many businesses that handle credit card transactions give the customer the option to store the information for later use as a convenience, which means the stored information is a target for potential threat agents. Thus even businesses whose primary function is not financial must be concerned with computer security.

To be successful, most of these examples of fraud and theft would require detailed knowledge either from an internal employee or through careful reconnaissance. However, many businesses and individuals do store common types of data. This data might include usernames, passwords, customer information and payment information. Usernames can be retrieved relatively easily through null sessions (Details), and passwords can be discovered by several methods including recording keystrokes, reading password caches (Gutmann, "How"), and capturing unencrypted data from the network. People are often not security conscious, and may reuse the same password for multiple systems, thus, a single captured password may yield access to multiple systems. Threats from captured data may not be immediate. A threat agent may wait until the target has a false sense of security and then return to try the captured authentication information.

Financial information is not the only valuable information that businesses may retain in their computer systems. Human resources databases are packed with personal information. Often this may include social security numbers, home

address, income and dependants. Individuals who use computers for home use may also be targets. Large amounts of information are stored in personal finance packages such as Quicken. Personal information may be valuable to criminals because personal information can be used in identification fraud (United States, Dept. of the Treasury, Comptroller).

Computers can also provide a medium for extortion. In business, this could be a threat agent encrypting all the data necessary for a business's livelihood and holding the data for ransom (United States, "Hacker Raid"). Individuals might also be affected by an extortion scheme. An threat agent could upload or steal data from an individual's hard drive that may be illegal or embarrassing, and then black mail them with the knowledge.

Computers may also be used for sabotage. For instance, a threat agent could modify medical records (Fischetti; "Hacker Gains") to cause a doctor to make a false diagnosis, or to prescribe an overdose. The possibility even exists that harm could come to a person from the other side of the world. Many types of valuable information exist on both business networks and personal computers that may be valuable.

The Value of Personal Information

Personal information may not seem valuable. Yet, personal information is necessary to commit identification theft and fraud. A simple case of fraud may be stealing enough information to make fraudulent charges on credit card, or a fraudulent withdrawal from a bank account. More complex theft and fraud may include procuring credit cards, bank account, utility service, and loans in someone else's name (United States, ID).

Personal information can also be used to obtain legal documents such as passports and driver's licenses. Criminals have even been known to give police false information, thus leading to a permanent association between an innocent person and a criminal's activities. For instance, police can track credit card numbers used to purchase illegal goods or services ("Mass arrests"). If a stolen identification and credit card information are used, the police might arrest an innocent person.

Valuable information useful for identification fraud includes account numbers, Social Security number, name, address, phone number, birth date, employment information, amount of income, and mother's maiden name (United States, ID). Using this information a criminal can provide false information to pass criminal background and credit checks, which in turn may allow them to obtain a position of trust. Thus, stolen information can be of great value to criminals both financially, for obtaining trust, and for misleading investigations.

How the Perimeter Defenses Will Be Penetrated

Most businesses and an increasing number of consumers access the Internet. Controlling which information can enter and leave the network can be challenging, and threat agents are aware of these challenges. Consumers often

need to initiate a connection from their computer to a business. Businesses need to give customers access to the products or services they make available via the Internet. Additionally, employees and business processes often require access to resources externally available on the Internet. With the increasing popularity of web services, gathering information in real time from a variety of diverse sources external to the business will create additional network traffic that a threat could hide in.

Many services such as SMTP and HTTP pass through perimeter defenses such as a firewall without any authentication. Some proxy level firewalls can provide authentication of services, but often authentication and content filtering are left to the application providing the service, such as a web server. Services for remote users and vendors present another point of entry via virtual private networks and modems. Modems might be connected directly to servers for remote vendor access. Businesses often buy blocks of phone numbers, thus enabling modems to be found more easily. Virtual Private Networks provide a method to access services through an encrypted tunnel (Mactaggart). If a malicious program is residing on a remote user's computer, then the malicious program will have the same access as the user has through the tunnel. Filtering and virus scanning are important not only for untrusted sources but also for trusted sources that access systems via encrypted tunnels. Although tunnels may be authenticated and encrypted, that does not mean the data that traverses the tunnel is safe.

How the Threat Agent Will Avoid Detection

Many network intrusion detection products, which rely on observing unencrypted communications, may be blind to the same threat that occurs via an encrypted data stream. For instance, SSL provides a method to encrypt a data steam to ensure confidentiality and integrity of the data stream (Mactaggart). Thus, a threat agent could perform an attack via an SSL encrypted data stream, and the network intrusion detection software would not be able to observe the threat because the data stream is encrypted. A situation is even conceivable where a virus utilizing some sort of encryption, possibly S/MIME, could evade virus scanning at a central mail gateway.

The avoidance of detection applies not only to malicious code and attempts to penetrate the perimeter, but also to internal employees and malicious code that may be attempting send valuable information out of the internal network. Therefore, content filtering and traffic filtering software should filter outbound traffic as well as inbound traffic.

Other threats exist internally, such as modifying logs, in order to remove evidence of an attack or falsifying log messages so that the attack will be overlooked (bELFaghor). Further, network based intrusion detection products are often tuned to report on only a subset of the total traffic. Therefore, communicating on one of the unmonitored subsets may also avoid detection. Additionally, poor placement of network intrusion detection systems may neglect network traffic that originates on the internal network. If an employee initiated the

threat or if an internal system has been subverted, and threats originate from the internal network, then these threats may not be detected if intrusion detection is only monitoring the perimeter systems.

Similarly, some anti-virus products scan only files of a specific type. Recent viruses such as WineVar can evade this selective scanning by registering new file types ("WineVar"). Steganography provides another means to avoid detection. Confidential information could be posted on a company's web site by encoding the information in a picture. Additionally, other documents, such as word documents or even harmless looking E-mails can have information encoded in them. Although an internal networks may use address ranges recommended by RFC 1597 (Rekhter), that neither prevents the flow of information into or out of those networks, because network address translation can occur. Since a potential threat may come from an internal source, restricting access between internal systems through network and host based access controls may also be a prudent step. Thus content filtering, traffic filtering, and intrusion detection are important not only at the perimeter, but also within the internal network.

The Role That Social Engineering Plays in Threats

Social engineering can play a significant role in enabling the installation of malicious code. This was demonstrated by malicious and nuisance code such as the I Love You email virus and the mass mailer from FriendGreetings.Com ("2002"). This code relies on emotions such as trust, lust, and curiosity. Fortunately, due to the high volume of unsolicited E-mail people receive, they might be less likely to open E-mail from an unknown sender. Social engineering can also take the form of a threat agent communicating directly with the target. The threat agent might E-mail or call the target and claim to be technical support person that needs their assistance. The threat agent might then request a password or ask the target to execute a piece of malicious code. This can also take the form of a threat agent gaining physical access an internal network. A threat agent, for instance, could follow a group though a door as they return from a break. A good security policy combined with employee education can help prevent these threats.

What Happens When the Threat Agent Gets Administrative Privileges

Root, on Unix and Unix like operating systems, and Administrator, or the various Administrative groups on Microsoft operating systems, have limitless power. A program running with these privileges can modify installed programs and registry keys, and can install new programs, device drivers and kernel loadable modules and possibly access the firmware and hardware directly. Most frightening of all, with administrative permissions a malicious program can violate the Trusted Computing Base and the reference monitor (Frost) through which all authorization requests pass. Once the Trusted Computing Base and reference

monitor have been modified or bypassed, reinstallation of the operating system may be necessary to reestablish provable integrity of the system.

Imagining Possible Threats

An Information Relay. A relay could execute on a mobile user's computer while their VPN is in use. The relay could send data between the threat agent on the Internet and the user's private network accessible by the VPN. Thus, the threat agent could access anything that would be accessible to that user via the VPN.

A Reverse Server. A program which initiates a connection from inside the internal network to the external network, possibly using valid HTTP ("Reverse") to avoid filtering by a proxy firewall, and then accepting commands from the remote computer it connects to. This is possible because many organizations are much more willing to allow employees access to some of the Internet or the entire Internet without restriction.

Dynamically Loadable Modules. Dynamically loaded modules might include new methods to communicate information, new target information to search for or a method to exploit the most recent vulnerability information. A Root Kit acting as part of a distributed peer-to-peer network could dynamically update its self to exploit vulnerabilities before the system administrator has had a chance to patch the system. Sidedoor.cpp is one such example of this threat ("Sidedoor.cpp").

Root Kits. Root kits for Unix and Windows (Hoglund) violate the Trusted Computing Base (Frost), and are thereby able to hide themselves and their activity. Activities include replacing or augmenting any part of the operating system. Intercepting system calls, for instance, can reveal passwords and private keys. Knark is an example of a root kit that can hide itself from the process table, Netstat and even avoid detection by integrity checking tools like TripWire (Creed). A root kit could also employ a method similar to the Bolzano virus to bypass the reference monitor so that no authorization is enforced (Paddingx). Because root kits can intercept system calls, they can hide from or disable virus scanners. In theory, a root kit would be loaded into memory whenever the operating system was loaded into memory. Thus, the root kit would only be detectable if the root kit does not affect the operating system or virus scanning software scanning the affected volume. This would require mounting the affected volume as a non boot device via a non-compromised system, so that the results of the scan will be reliable. Further, stolen keys could threaten nonrepudiation. A stolen private key could be used to forge messages, or sign binary code (Gutmann, Format). A stolen private key could even be used to falsify legally binding documents because electronic signatures are legally binding ("Electronic").

Anonymous Communications. The program either is controlled by an anonymous source or posts the data that it harvests to an anonymous source.

This may include Internet Relay Chat, Instant Messaging, Email, Web Logs (Blogs) or more complex anonymous relays such as six/four (Mixter) and FreeNet (FreeNet). Anonymous communications provide little or no means to identify the consumer of the information.

Encryption. Communicating via encryption can prevent a Network Intrusion Detection (NID) system from monitoring the content of the data stream, and it could also be an effective way to inject signed modules into a virus engine. A threat might also try to steal or sign its self with a certificate used to sign trusted content (Gutmann, Format).

Kernel Level Access to the Network. With kernel level access to the network a program can listen for incoming packets without opening a connection that could be detected by a port scan. Evidence that the root kit is listening to network traffic would not be shown using a program like Netstat to view network statistics ("Cd00r.c"). The root kit could communicate with other compromised nodes by sending packets in a seemingly non-coherent data stream. The non-coherent data stream could randomize the port, source and destination address or other parts of the packet, if the listener was still able to capture the packets. This may even evade NID products that monitor specific ports and data streams. Another use might be to establish a heartbeat with compromised neighbors that could determine if counter measures are being taken. Because the root kit can see all the packets that are sent to the network interface, it could also intercept passwords or other sensitive data. Even in a switched environment where packets are sent to ports associated with specific MAC address, it is possible to view packets using techniques such as those employed by Dsniff to flood the switch's MAC address table. Another possible method is forging Address Resolution Protocol (ARP) packets to poison the ARP cache (Altering). ARP maps between an IP address and a MAC address. A router examines the destination IP address in a packet and then attempts to forward the packet to the next hop router's MAC address, or to deliver the packet to the final destination's MAC address. A poisoned ARP cache could result in the packet being delivered to a threat agent's MAC address. This misdirection would allow the data stream to be intercepted. Another possibility is simulating dynamic routing protocol updates. This method could either reroute traffic past the compromised node's interface or discover the address ranges of other parts of an internal network.

Cross Platform. Cross platform code can take many forms. These forms include scripting languages, such as VBScript or Perl, or byte code, such as Java, or encapsulated binary data or source code. Scripts can function wherever a suitable interpreter exits. Byte code requires a just-in-time compiler or virtual machine to execute the byte code. Encapsulated binary data, for the appropriate platform, can be written to a file, enabling the program to create an executable file. Source code can be complied into a native application binary if a compiler is installed.

Data Hiding and Steganography. Simple data hiding can take many forms. On a FAT file system it may take the form of invisible directory names, such as names composed of the ASCII character 255. On NTFS, file systems invisible files may use alternate data streams, which do not appear in the file system. On Unix, file systems, a directory might be given the name period-space. On Unix file systems, files that begin with a period are normally not listed in a directory listing and white space is normally used as a token separator. Further the file named Period references the current working directory. This can also take the form of putting information in parts of files that are not accessed or viewed. For instance, placing data in the comment tags of an HTML document would likely go unnoticed. Another example is to create a file that is both a graphical image and a zip archive. More complex forms of data hiding such as Steganography can also be employed. Steganography can take many forms. A program could hide information in a text based document by changing letters at specific intervals. Information could be hidden in a graphic image by slightly changing the image so that the changes are not visible to the human eye. Information could also be hidden in plain sight by generating a coherent story with embedded patterns. Files could be hidden within files (Steganography). Information can even be hidden in a binary program without changing the function or size. Hydan is an example of a program the can change binary files in this way (Crazyboy). A root kit could act at the file system level, possibly in a manner similar to Rubber Hose (Rubberhose). Any program that can modify files can hide information in them. This also presents another way for a malicious program to communicate. The program can either receive instructions by loading an image from a web site somewhere on the Internet or disseminate information by embedding the information in an image posted on a publicly accessible web site. The trade secrets of a company could be placed on their own web site without them even noticing.

Delayed Activation. Programs that hide themselves and delay their activation might be written to a backup tape, thereby poisoning the backup. Even if the program is removed, the program could be inadvertently restored when the backup is restored. The program may also lie in wait until a user with administrative privileges executes the program. In other words the program may wait until the probability for success is optimal.

Rapid Spreading. As discussed in How To 0wn the Internet In Your Spare Time (Staniford), there are several ways to increase the rate at which automated code could spread throughout the Internet or an internal network. These methods include efficient detection of vulnerable services on targets, detection of already compromised hosts, and searches of the address space in an efficient and non-random way. Attacks targeted at internal networks, possibly even released by an internal employee, could infect even the largest corporation in hours or minutes.

Prevention and Detection of Internal and External Network Threats

This paper has presented several groups of people, their possible motivations and some of the techniques they might use. Different individuals and businesses have different potential risks. Further, the value of the assets protected by reducing risk will vary greatly among different individuals and different businesses. Therefore, each will need to perform a cost benefit analysis. This section looks at few ways to reduce risks.

Physical security of a bank might be very different from the physical security of a small business. Some common physical security mechanisms might include bulletproof glass, emergency buttons to call the police or the fire department, a guest sign in log, access badges, biometrics, security guards, and security cameras. Policies might also regulate the movement of guests and vendors, such as requiring them to be escorted. Restrictions might also limit which devices employees are permitted to bring into the office. Portable devices like cell phones, pagers, and personal digital assistants might enable sensitive information to be stored or transmitted, as well as present a potential entry point for threats such as malicious code. Policies regarding which information can enter and leave the facility may also be put in place. This could ensure that employees can't walk out the door with a binder full of trade secrets, and might also ensure the confidential materials are properly destroyed before being discarded.

Security can start with the hiring process. This might include effective screening methods to identify an individual's risk factors for committing a crime (Plotkin; Jones). Effective employee screening techniques might include credit checks, criminal background checks, finger printing, reference checks, and psychological screening. Psychological screening might include techniques such as integrity testing to evaluate how an employee reasons through complex ethical dilemmas to help determine their ability to rationalize theft.

Education can play a significant role in security. Those responsible for security should keep their knowledge current with regard to appropriate ways to build and secure systems and networks. In addition to taking classes, consider subscribing to relevant notification services to keep abreast of the new threats, and what can be done to avert them. The Security Focus Bugtraq forum is an example such a service. Proper employee education is in important also. Not only should employees be aware of the security policies so that they can obey them, but employees may be the first to notice internal attempts at fraud or theft. For instance, a policy might encourage employees to report any suspected theft or fraud activity.

Project planning, change control, and disaster recovery are important for ensuring integrity. Analyzing projects early in the planning stage can help to prevent possible fundamental security design flaws. Detailed change control might have multiple benefits. One of which is detailed documentation. Another is that well documented changes can help identify the cause of issues that may affect confidentiality integrity, availability or a combination of those. Disaster

recovery is important in the event that some data becomes corrupt or is destroyed. Good rotation and retention policies may be necessary to so that backup media can be removed from the rotation cycle. This is important in the event data becomes corrupt and the corruption is not noticed for weeks or months.

System maintenance can be critical to maintaining availability. The mean time between failures may be able to be estimated based on the mean time between failures of the system's components. Using statistical failure estimation techniques, spare parts predicted to fail could be kept immediately available when the probability of failure is sufficiently high.

Similarly, staying current with the most recent patches will become increasingly important. In some cases, code to exploit a vulnerability is released less than a day after the announcement of a vulnerability. Patching in a timely manner is further reinforced when there is the possibility that a malicious program released by an internal employee or by someone on the Internet could spread to all targeted systems in less than a day.

As threats become more complex and harder to detect, distributed statistical analysis of network traffic will become an increasingly useful tool. Correlating information for statistical analysis implies that all the data is centrally correlated, such as a server that aggregates all of the log files for a business. Dshield already performs a service like this for the Internet by analyzing log files. Statistical analysis tools such as Dshield will become increasingly useful on large corporate networks as well. On large internal networks, traffic patterns may be much more consistent. This, in turn, would allow for easier detection of anomalous behavior. Effectively establishing a baseline for correct system behavior is also important. If a baseline is taken after a system has been compromised, then the network traffic resulting from the compromise will not appear to be anomalous. Another method to detect anonymous activity may be to use a honey pot or some form of bait. For instance a bait file or server could be monitored for access. Early detection of anomalous network activity caused by reconnaissance may help to identify the threat before any damage is done, especially if the threat agent is an internal employee or vendor.

Multiple layers of filtering can be an effective deterrent. Many businesses already have perimeter firewalls, but supplementing those with host based firewalls and additional network firewalls can reduce risks. Individual workstation and servers can control the flow of their inbound and outbound network traffic with programs such as TCP Wrappers, IPFilter, the PF packet filter, or personal firewall software. Packet data such as the source or destination port, source or destination address, and fragment reassembly can be filtered. Additional packet filtering can also be added to the network. This might include enabling the packet filter features of a router that is already in place, or a new firewall might be needed. Often, firewalls separate different parts of a network by acting like a router. Some firewalls, such as the OpenBSD PF packet filter, are capable of filtering network traffic while acting as a layer two device, like a bridge or a switch (OpenBSD). These inline or bridging firewalls can be placed into an existing network relatively easily, and may even be more secure that a traditional firewall.

They may be more secure because the interfaces can be configured without an IP address. Thus, the inline firewall is as invisible as a switch. Personal firewalls can help protect mobile users and prevent a VPN from being used as a relay. Additionally, on a local area network, personal firewalls can ensure that workstations only communicate with the necessary services and servers. Proxies can also be effectively used on firewalls to validate data streams and limit the size of requests, which can help prevent buffer overflows.

Separation of data can be critical for ensuring confidentiality and integrity. For instance, data streams can be encrypted using protocols such as Secure Socket Layer (SSL), Secure Shell (SSH), and IP security (IP Sec. VPNs). This may not only be useful to prevent data sent over the Internet from being intercepted, but also for securing data on an internal network. A layer of encryption can be added to legacy applications that send sensitive data in an easily decoded form. Software providing encrypted tunneling services includes Stunnel, OpenSSH, IP Sec. VPN implementations on Linux and OpenBSD, and many commercial products that provide these services. Resources can be separated between servers, in such a way that all confidential information is separated from information that is not confidential. File system access controls can be employed to selectively control access. Data can also be encrypted to control access to the data. Encryption might occur at the file system level encrypting whole files or whole file systems. Encryption could occur at the record level, encrypting individual elements of a database or spreadsheet. Encryption combined with cryptographic hashes, provide a method to ensure that data has not been modified. Integrity checking tools such as TripWire employ this technique. Gnu Privacy Guard, and the Gnu Privacy Project provide the ability to encrypt files and establish nonrepudiation of E-mail.

Removing unused executable files and unnecessary permissions can reduce risks. Each piece of code residing on a users computer could contain an as of yet undiscovered vulnerability. If reducing the risk is too expensive, buying insurance or requiring vendors, such as custodial staff, to be bonded, could also shift the remaining risk.

Risks can also be reduced through separation of duties. Effective separation of duties prevents complex frauds from taking place that involve modification of records (Small). Separation should be addressed not only for operational duties such as ordering and accounting for inventory, but also system administration duties such as auditing access logs and granting access. Separation of duties combined with regular auditing might help to detect the kind of sabotage that happened at UBS PaineWebber (Lemos).

Conclusion

As laws and defenses improve, threats in the future are likely to be targeted at specific data of value. The most devastating threats are most likely to occur from employees or people familiar with the inner workings of a company. The effects of threats may not be isolated to individual servers or applications. Rather, the effects may spread rapidly throughout a network. Whether for

revenge or greed, the threats of the future will be serious and devastating. Companies risk losing money directly from downtime, cleanup, and repairs caused by the threat. Additionally, after the immediate monetary loss, the company may suffer the consequences of lost customer confidence. Further, the threat is not limited to businesses. The potential exists for an automated way to quickly harvest all the personal data available from consumer's computers directly connected to the Internet. For a business, the careful combination of multiple defensive layers, thorough baselining, detailed auditing, effective incident response, limited access, education, and shifting the remaining risk can reduce risks to an acceptable level. Consumers may be equally threatened, but much less prepared and much less aware of their risks. As businesses increase their security, perhaps a trickle down effect to consumers will occur.

Works Cited

"2002 Malware Review: Virus Writers Contribute to SPAM." 22 Dec. 02. About.com. 28 Mar. 2003. <http://antivirus.about.com/library/weekly/aa122202a.htm>.

Altering ARP Tables (version 1.00). 2001. DataWizard. 25 Mar. 2003 <http://packetstormsecurity.nl/papers/general/Altering_ARP_Tables_v_1.00.htm>

Anley, Chris. Advanced SQL Injection In SQL Server Applications. 31 Jan. 2002 Next Generation Security Software Ltd. 14 Mar. 2003 <http://www.nextgenss.com/papers/advanced_sql_injection.pdf>

bELFaghor. "SYSLOGD." BFI Feb 1999. 28 Jan 2003 <http://www.s0ftpj.org/bfi/online/bfi5/bfi5.09.html>

Boulanger, A. "Catapults and grappling hooks: The Tools and Techniques of Information Warfare." IBM Systems Journal. 37.1. (1998). 18 Jan. 2003. <http://www.research.ibm.com/journal/sj/371/boulanger.html>.

Bowman, Lisa. "Professor to Delve into Anti-copying Flaws." CNET News.com 14 Aug. 2001. 21 Mar. 2003. <http://news.com.com/2100-1023-271631.html>.

Brehm, Sharon, and Saul Kassin. Social Psychology, Third Edition. Boston: Houghton Mifflin, 1996

"Cdoor.c . Packet Coded Backdoor." Packetstormsecurity.nl. 13 June 2000. 3 Mar. 2003. <http://packetstormsecurity.nl/UNIX/penetration/rootkits/cd00r.c>.

Chien, Eric, and Péter Ször. Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques in Computer Viruses. 2002. Symantec Corporation. 09 Dec. 2002 <http://securityresponse.symantec.com/ avcenter/ reference/ blended.pdf>

Council of Europe. Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Transborder data flows. 08 Nov. 2001. 02 Apr. 2003 <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=181>

---. Convention on Cybercrime. 23 Nov. 2001. 02 Apr. 2003 <http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185>

Crazyboy Home Page. 16 Mar. 2003. <http://www.crazyboy.com/hydan/>.

Creed. "Knark v 0.59." Packetstormsecurity.nl. 4 Feb. 2001. 3 Mar. 2003. <http://packetstormsecurity.nl/UNIX/penetration/rootkits/knark-2.4.3.tgz>.

Details About NULL Sessions. 28 Jun. 1999. NT OBJECTives, Inc. 11 Mar. 2003 <http://downloads.securityfocus.com/library/null.sessions.html>

European Union. Network and Information Security: Proposal for a European Policy Approach. 1 Feb. 2003. <http://europa.eu.int/information_society/eeurope/news_library/pdf_files/netsec_en.pdf>.

"FBI Arrests Programmer in Las Vegas.". Electronic Frontier Foundation. 17 July 2001. 02 Apr. 2003 <http://www.eff.org/IP/DMCA/US_v_Elcomsoft/20010717_eff_sklyarov_pr.html>

Fischetti, Mark. "Helpful Hacking." IBM Think Research. 10 Feb. 2003. <http://domino.research.ibm.com/comm/wwwr_thinkresearch.nsf/pages/hacking397.html>.

The Freenet Network Project. 26 Mar. 2003. 16 Mar. 2003. <http://freenet.sourceforge.net/tiki-index.php>

Frost, James. "Building Secure Systems I: TCBs, Reference Monitors, Protection Domains, Subjects and Objects." Pocatello, Idaho, 17 Feb. 2003. 23 Mar. 2003. <http://cob.isu.edu/cis410/week4.htm>.

Gordon, Sarah. "The Generic Virus Writer." IBM Research. Sept. 1994. 1 Feb. 2003. <http://www.research.ibm.com/antivirus/SciPapers/Gordon/GenericVirusWriter.html>.

---. "Technologically Enabled Crime: Shifting Paradigms for the Year 2000." IBM Research. May 1994. 20 Mar. 2003. <http://www.research.ibm.com/antivirus/SciPapers/Gordon/Crime.html#SOCIAL>.

Gutmann, Peter. Format of a Signed File Page. Dept. of Computer Science, U of Auckland. 20 Mar. 2003. <http://www.cs.auckland.ac.nz/~pgut001/pubs/authenticode.txt>

---. "How Windows encrypts .PWL files." Online Posting. 28 Nov. 1995. 28 Mar. 2003 <http://www.cs.auckland.ac.nz/~pgut001/pubs/pwl.txt>

"Hacker Gains Access to 7,000 Patient Files in Indianapolis." SC Infosecurity News: The Information Security Portal. 10 Mar. 2003. 20 Mar. 2003. <http://www.infosecnews.com/sgold/news/2003/03/10_05.html>.

Hoglund, Greg. "A Real NT Rootkit." Phrack Magazine 9.55 (1999). <http://www.phrack.org/show.php?p=55&a=5>.

Jones, John W. and David W. Arnold "Trends in Personnel Testing: A Loss Prevention Perspective." Loss Prevention Journal. 25 Feb. 2003, <http://www.losspreventionjournal.com/articles/321feat2.html>.

Kehoe, Brendan. "The Robert Morris Internet Worm." Zen and the Art of the Internet. Jan. 1992. 12 Feb. 2003. <http://www.swiss.ai.mit.edu/6805/articles/morris-worm.html>.

Krause, M.S. "Contemporary White Collar Crime Research: A Survey of Findings Relevant to Personnel Security Research and Practice." The Personnel Security Managers' Research Program. Aug. 2002. 14 Mar. 2003 <http://www.navysecurity.navy.mil/White%20Collar%20Crime.pdf>

Lemos, Robert. "Ex-IT worker charged with sabotage." CNET News.com. 18 Dec. 2002. 03 Mar.2003. <http://news.com.com/2100-1001-978386.html>.

Loss Prevention Guide. 2000. ADT Small Business Loss Prevention Center. 20 Feb. 2003. <http://www.adt.com/divisions/small_business/loss_prevention_center/guide/internal_theft.cfm>.

Mactaggart, Murdoch. "Introduction to cryptography, Part 4: Cryptography on the Internet." IBM Developer Works. Mar. 2001. 04 Mar. 2003. <http://www-

106.ibm.com/developerworks/security/library/ s-crypt04.html?dwzone=security>.
"Mass arrests over online child porn." BBC News. 20 May 2002. 15 Feb. 2003. <http://news.bbc.co.uk/1/hi/uk/1998515.stm>.
Mannes, George. "Cracking the Books II: Reliving Equity Funding, the Cal Ripken of Stock Funds." TheStreet.com. 22 Oct. 1999. 25 Mar. 2003. <http://www.thestreet.com/stocks/accounting/789337.html>.
McCallaugh, Declan. "Letter to Secure Network Operations, Inc." 29 July 2002. 31 Mar. 2003. <http://www.politechbot.com/docs/ hp.dmca.threat.073002.html>.
Mixter. Announcement of the Six/Four System Page. 22 Mar. 2003. <http://mixter.warrior2k.com/h2k2speech.txt>.
OpenBSD Bridging Firewall Configuration. 26 Sep. 2002. Computer Facilities Management group, University of Washington. 15 Mar. 2003 <http://cfm.gs.washington.edu/security/firewall/pf-bridge/>
Oppenheim, Matthew. "RIAA/SDMI Legal Threat Letter." Letter to Professor Edward Felton. 9 Apr. 2001. 03 Mar. 2003. <http://www.eff.org/ Legal/Cases/Felten_v_RIAA/20010409_riaa_sdmi_letter.html>.
Paddingx. "Work in Progress (4)." Online Posting. 28 Jul. 1999. 09 Dec. 2002 <http://groups.google.com/groups?selm=01bf39c9%2464e37060%249db0 95c2%40defaut&oe=UTF-8&output=gplain>
Plotkin, Harris. "Methods of Identifying Dishonest Employees: Minimizing Worker Theft, Fraud, and Embezzlement. Loss Prevention Journal. 25 Feb. 2003. <http://www.losspreventionjournal.com/ articles/ 231feat2.html>.
Poulson, Kevin "'T0rn' Arrest Alarms White Hats, Advocates." Businessweek.com. 25 Sept. 2002. 19 Feb. 2002. <http://www.businessweek.com/technology /content/ sep2002 /tc20020925_0548.htm>.
Rekhter, Y., T.J. Watson Research Center, B. Moskowitz,. D. Karrenberg, G. de Groot. "Address Allocation for Private Internets." RFC.net. Mar. 1994. 5 Mar. 2003. <http://rfc.net/rfc1597.html>.
"Reverse WWW Tunnel Backdoor." Securiteam.com. 3 Aug. 2002. 03 Mar. 2003. <http://www.securiteam.com/tools/5WP08206KU.html>.
Rubberhose Home Page. 03 Mar. 2003. <http://www.rubberhose.org/>.
Sieber, Ulrich. "Legal Aspects of Computer-Related Crime in the Information Society COMCRIME-Study." Ms. 1 Jan. 1998. 03 Mar. 2003. <http://europa.eu.int/ISPO/legal/en/comcrime/sieber.doc>.
"Sidedoor.cpp." harmony.haxors.com. 15 Mar. 2003. <http://newdata.box.sk/ 2001/okt/sidedoor.cpp>.
Small Business Advisor: Financial Fraud. May 1999. Napier & Company: CPA and Business Consultants. 21 Mar. 2003. <http://www.napiercpa.com/ newsletter/mar99/page2.html>.
The SMB Proxy Tool Page. 25 Mar. 2003. <http://www.cqure.net/ tools.jsp?id=02>.

Staniford, Stuart, Vern Paxson, and Nicholas Weaver. "How to Own the Internet in Your Spare Time. Proceedings of the 11th USENIX Security Symposium. 23 Feb. 2003. <http://www.icir.org/vern/papers/cdc-usenix-sec02/>.

Steganography Wing of the Gallery of CSS Descramblers. 15 Mar. 2003. <http://www-2.cs.cmu.edu/~dst/DeCSS/Gallery/Stego/index.html>.

"Digital Millenium Copyright Act." Thomas: Legislative Information on the Internet 28 Oct. 1998. 11 Mar. 2003. <http://thomas.loc.gov/cgi-bin/bdquery/z?d105:HR02281: @@@T|TOM:/bss/d105query.html>.

"Electronic Signatures in Global and National Commerce Act." Thomas: Legislative Information on the Internet . 30 June 2000. 16 Feb. 2003. http://thomas.loc.gov/cgi-bin/bdquery/ z?d106:SN00761 :@@@T|TOM:/bss/d106query.html>.

"Gramm-Leach-Bliley Act". Thomas: Legislative Information on the Internet. 12 Nov. 1999. 11 Mar. 2003. <http://thomas.loc.gov/cgi-bin/bdquery/z?d106:SN00900:| TOM:/bss/ d106query.html>.

"Health Insurance Portability Bill." Thomas: Legislative Information on the Internet. 21 Aug. 1996.. 11 Mar. 2003. <http://thomas.loc.gov/cgi-bin/bdquery/ z?d104:HR03103:|TOM:/ bss/d104query.html>.

"USA PATRIOT ACT Act of 2001." Thomas: Legislative Information on the Internet 26 Oct. 2001. 11 Mar. 2003. <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:@@@T|TOM:/ bss/d107query.html>.

United Kingdom. Her Majesty's Stationery Office. Computer Misuse Act 1990 (c. 18). 05 Mar. 2003. <http://www.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm>.

United States. Dept. of Justice. 18 U.S.C. Fraud and Related Activity in Connection with Computers. 24 Jan. 2002. 9 Feb. 2003. <http://www.usdoj.gov/criminal/cybercrime/1030_new.html>.

---. ---. Computer Crime and Intellectual Property Section (CCIPS). Press Releases. 2003. 29 Mar. 2003. <http://www.usdoj.gov/>.

---. Dept. of State. Bureau of Diplomatic Security. "Hacker Raid: Key Server Stripped: 'It Was Akin to Hacking Into The Pentagon." National Post's Financial Post & FP Investing. 24 Feb. 2003. 3 Mar. 2003. <http://www.ds-osac.org/view.cfm?KEY=7E4454404050&type=2B170C1E0A3A0F162820>.

---. ---. ---. "Cyber-crime Reporting on the Increase." VNU Business Publishing. 24 Mar. 2003. 27 Mar. 2003. <http://www.ds-osac.org/view.cfm?key=7E4457444753&type=2B170C1E0A3A0F162820>.

---. Dept. of the Treasury. Comptroller of the Currency Administrator of National Banks. How to Avoid Becoming a Victim of Identity Theft. 16 Feb. 2003. <http://www.occ.treas.gov/idtheft.pdf>.

---. ---. ID Theft: When Bad Things Happen to Your Good Name. Sept. 2002. 14 Mar. 2003. <http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.pdf>.

"WineVar Redefines Executables: Simple Technique May Have Far-Reaching Implications." About.com. 25 Nov. 2002. 28 Feb. 2003. <http://antivirus.about.com/ library/weekly/ aa112502a.htm>.