Global Information Assurance Certification Paper

Christopher Hillas
GSEC 1.4B Option 1
June 5, 2003

Authentication and Control of Remote Connections

Abstract:

An often over looked weak link in today's network environment are modems. Remote connectivity can make life easier for support of remote servers, but the technology can generate vulnerable avenues that threaten to put today's seemingly secure servers at a high risk. There is possibility of attacks against analog tones used by modems to authenticate. Once a user is authenticated there is a possibility of a remote attack against the stand-alone host server or rest of the environment. Once a remote connection is initiated the types of attacks can be the spread of a virus or Trojan like the SQL Slammer. This risk can be reduced with better authentication and control of modem connections. There is no perfect solution to protect an environment. A best-case scenario is a combination of solutions to reduce any signal point of failure through out the modem connection. The types of modems this document is centered on are 56k modem devices that connect to the publicly switched telephone service networks. These principles required to secure a 56k modem can apply to other modem types like ISDN modems, Cable modems, or DSL modem technologies as well. The servers addressed are Microsoft Windows 2000 servers with a current patch revision level. Further, this paper assumes that adequate virus protection is in place on the server.

It is important to eliminate the certainty of risk that a modem will introduce before the threat of an attack becomes a reality. For example, there is no risk of death to go for space walk without a space suit because an astronaut would die. Undoubtedly, modems, like the unprotected space walk are bad choice. A production machine with a modem needs third party tools to protect, track, and authenticate connections from a modem. There are numerous answers and combination of solutions that reduce the vulnerabilities of modem connections. Thus, security needs to be implemented on the server to protect the server and networked environment from modem risks. These strategies need to reduce modem risk of poorly authenticated and insecure connections. Also, multiple means to track the activity that transpires from a remote connection to the server and the rest of the environment are necessary to protect the environment. There will always be a need in distributed client server environment for remote access, but this access needs to be secure and without a high level of risk. Successful security must provide redundant solutions to the risks modems present by limiting threat levels to an acceptable level or provide alternative actions to insecure technology like a modem.

Paper:

An often over looked weak link in today's network environment are modems. Remote connectivity can make life easier for support of remote servers, but the technology can generate vulnerable avenues that threaten to put today's seemingly secure servers at a high risk. This risk can be reduced with better authentication and control of modem connections. There is possibility of attacks against analog tones used by modems to authenticate. Once a user is authenticated there is a possibility of a remote attack against the stand-alone host server or rest of the environment. Once a remote connection is initiated the types of attacks can be the spread of a virus or Trojan like the SQL Slammer. There is no perfect solution to protect an environment. A best-case scenario is a combination of solutions to reduce any signal point of failure through out the modem connection.

The types of modems this document is centered on are 56k modem devices that connect to the publicly switched telephone service networks. These principles required to secure a 56k modem can apply to other modem types like ISDN modems, Cable modems, or DSL modem technologies as well. The servers addressed are Microsoft Windows 2000 servers with a current patch revision level. Further, this paper assumes that adequate virus protection is in place on the server.

A modem, as said by Search Systems 2002 article entitled "modem", "modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device." The types of modems this document is centered on are 56k modem devices that connect to the publicly switched telephone service networks though these principles of securing the connection can apply to other modem types like ISDN modems, Cable modems, or DSL modem technologies. Some of the most common justifications for modem use in a production environment are for remote access to systems for vendor application support, user file transfer, or for print and fax services. Unfortunately, these devices that make life easier can also create unnecessary dangers. This is because a modem on a server allows the server to pass data packets across the publicly switched telephone network. Thus, the modem connection circumvents much of the network security and can open up the server to attack vulnerabilities from a variety of malicious activity.

The first attack happens when a remote computer detects a telephone number that is assigned to a modem. This is accomplished either by dialing a single number at a time or with a program that can dial numerous telephone numbers. A war dialer is a simple application that allows users to dial numerous telephone numbers for the discovery of modem connections. This tool can automatically call a suite of telephone numbers and then record any modem responses to the calls. The war dialer then creates a log file of the newly discovered modem connections for an attacker to use at a later date. Robert J. Shimonski in his August 2002 work entitled "Hacking techniques, War dialing" warns that "a modem set to auto-answer will allow unauthenticated access from the PSTN (publicly switched telephone network) directly into your protected infrastructure." Before this happens an organization can detect any unauthorized modems in an environment by war dialing their own telephone suite of numbers. Thus,

war dialer attacks can be reduced with preventive scanning by system administrators for modems that are set to auto-answer.

Some war dialer tools like Toneloc are free and other war dialers are commercial such as Phonesweep 4.4. In the Phonesweep program a list of dialed telephone numbers are displayed on the left. When a connection occurs, the word connection is displayed next to the phone number will identify modems that are set to auto answer. Another way organizations attempt to limit the amount of war dialing attacks in their environment is by turning off the auto-response function so that the modem can not respond to calls. The idea is to reduce the threat so that only out going connections from the servers are made to servers outside of the network environment.

Unfortunately, turning off the auto-response setting of a modem will not protect the server. This is because any modem connection has a potential weakness in its authentication according to Hibbeln in his March 2002 article entitled "Capturing an Analog Modem Transmission." Hibbeln further states:

> "Modems that are faster than 2400 baud are full-duplex modems that talk to each other continually once a connection is established. This communication team can trade information regarding the quality of the line while negotiating the fastest and more reliable data rates. The negotiation results in two sets of customized transmit and receive amplitude and phase filter parameters, tuned to the line conditions of the moment in each direction. This means that someone can, with sufficient motivation, eavesdrop on an analog data call."

This then allows for the possibility of the attack form called "man in the middle." Hibbeln continues to comment:

> "This is difficult because, unless the third modem is electrically present at the beginning of the connection and is able to use the negotiation exchanges between the end-point modems, it cannot participate in the negotiation so it will have difficulty producing accurate data in real time. This would then establish a link for only one side of the connection because each end user uses different spectrum phases. Yet, a passive listening attack records audio from an analog phone line so that it can be demodulated into two data streams by post-processing with appropriate equipment. When this attack occurs, the attacker can then send data packets or read the clear text as if it was part of the natural hop of trusted endpoints."

In order to have a secure remote connection data may need to be encrypted before modem passes the data and authentication between computers must improve

A common misconception in achieving better authentication of remote connection is when the caller is dialed back too from the server. The dial back process is used to verify the origination of the connection. Unfortunately, this dial back feature is susceptible to another weakness in the architecture of modem technology that occurs before the signals are established. Phrack Seventeen, 07 April 1988, File 8 of 12 : "Dialback Modem Security" by David I. Emery states:

> "It is thus impossible to say with any certainty that when a modem goes off hook and tries to dial out on a line which can accept incoming calls it really is connected to the switch and actually making an outgoing call. And because it is relatively easy for a system penetrator to fool the tone detecting circuitry in a modem into believing that it is seeing dial tone, ringback and so forth until he supplies answerback tone and connects and penetrates system security should not depend on this sort of dial-back."

So for dial back to be successful the server should dial back on a separate phone line other than the one the remote call was made from. Emery continues to recommend, when possible, the dial out call should be made from a line that can not receive calls and can only dial out.

Fortunately for folks who find a reason to use modems, there are tools that can be used to reduce modem risks with third party tools that create layers of armor for the server. Essentially, modems need to have perimeter defense from remote attacks. Potential vulnerabilities in the modems because of weak authentication of the remote user and computer can be accomplished in many ways. The ability to track user activity can be achieved through various combinations of software designed for both authentication and logging of activity for stand alone and network servers.

The weakness of modem connections can be contained by better authentication. The first threat to authentication is ability to detect the telephone numbers that are used by the modems. Only those users who have rights to the server should have access to the modem number. The second weakness with modem authentication comes from the way the signals are passed between computers. This vulnerability can allow for the signal and data packets to be manipulated or listened to by an attacker. To overcome these risks in authentication tools like RSA tokens, Modem Pools, and IPSec can be deployed. These solutions should be considered to provide a well authenticated modem connection.

Many years ago, researchers like Diffie and Hellman theorized an authentication concept that has proven successful. Their idea is to combine something a user knows with something the user has to achieve authentication. This concept is realized by the key fob technology of the RSA Corporation. Authentication is achieved when a user's pass phrase (password) and a randomly generated six character pin are inputted as logon credentials. The pin is randomly generated by the LCD token fob every minute in coordination with the RSA authentication server. This combination limits the use of shared passwords because the user, with possession of the key fob, is the only one who can authenticate to the server. This solution has demonstrated to be successful in limiting the amount of shared or standardized passphrases in an environment. Unfortunately, the most common complaint with the key fobs technology is that the devices can fracture or brake too easily. Irregardless of this weakness, better authentication of modem connections can be applied down to the user level with the use of RSA token fobs.

A great solution to manage modem connections is a modem pool. This means that all modem modulation would not be configured on host by host bases but rather managed centrally. Modem pooling offers the ability to kick out a connection after an idle period has expired and absolute timeout that limits the total amount of time a

remote user can connect to the pool. User access to the modem pool can be limited to those departments that require remote access on an as needed basis. An example of this modem pool technology is offered by Equinox.

The Equinox modem pool solution is known as SpartCom. Most of the Microsoft desktop clients can use the SpartCom modem pool client that can create a virtual com port that directs the connection to the modem pool server. The server manages the external modem pool with SpartaCom's modem Pooling for Windows NT (MPNT) software that manages the Analog Modem Pool (AMP). An AMP such as the Equinox SST-64 when daisy chained together can support 128 modems through the signal Windows server. This authentication solution allows for granular management of user groups access to the modem pool. The modem pools can be assigned for specific users or groups that can split connections across the pool. The pool can block or manage incoming calls and define the time of day for outbound and inbound calls. Outbound calls can be tracked to specific users or departments for billing purposes. In this way there can now be a level of consistency for modem use in the whole organization. If this solution is implemented organizations need to still war dial their own environment to track and stop any unauthorized modem connections before they are violated by an attack.

Another way to architect good security into a modem connection is to create means of authentication via the protocols used by the connection. The open standard RFC 2401 known as Internet Protocol Security or IPSec allows for TCP/IP layer 3 encrypted tunneling between devices. The IPSec rules set are typically implemented for virtual private networks programs but the IPSec will work with modem communication to add value. In the Security Focus article from December 5, 2001 entitled "Using IPSec in Windows 2000 and XP, Part 1" Chris Weber states "IPSec provides authentication hosts before and during communications, confidentiality through encryption of IP traffic, Integrity of IP traffic by identifying modified or spoofed traffic, and prevention of replay attacks." The Authentication Header is independent of the IP Header. The AH contains information regarding the IP address of the original sender of the data packet without manipulating the data packet itself. The authentication of IP packets ensures the packets have not been changed. IPSec protocol can further add value by encrypting the data packets with a feature know as Encapsulating Security Payload (ESP). The ESP functionality builds off the Authentication Header and can not be used independent of AH. Unfortunately when ESP is used to encrypt the packet any malicious packets will also be encrypted. It is important to realize that the ESP feature may create a secure hacking channel. IPSec creates a secure channel of communication based on host identification that will not add latency to the network traffic. Authentication Headers feature of IPSec for validation of remote hosts may be the best gain with IPSec so that malicious packets can be stopped by other technologies such as a firewall.

Thus, there are many ways that add value to modem authentication of the remote users and computers. Though the success of RSA token fobs, modem pools, and IPSec add needed authentication of user and computer, there is still a need for organizations to track the activities of the user and their code once they have secured authentication to the server. There are further tools that track user activity on standalone server or in a networked environment. The best implementation would be

to combine these tools together for an effective multiple layer of defense. This is commonly referred to as “defense in depth,” which is analogous to the layers of an onion in the garden of security. When defense in depth is applied correctly it is difficult to ‘take a bite right out’ of it. Just as it is difficult to “take a bite right out” of an onion because there are so many layers of the onion to get through. Thus, when defense in depth is applied there is no single point of failure on a system for malicious activity to occur. For example, the process of hardening the operating system is based on computer industry best practices analogues to adding layers to the onion. The use of utilities such as Hfnetchk, Windows Update and Microsoft Baseline Security Analyzer are a common implementation of defense in depth for patching the operating system vulnerabilities. Also implementing computer industry best practices found at sites like “www.corp-sec.net.” can demonstrate other ways to securely configure a host operating system. This concept of defense in depth can further prevent malicious activity from occurring on a server.

Over the years many tools have been developed that can stop, and log unwanted activity to protect the server. Examples of these tools that can prevent malicious activity are firewalls, host based intrusion detection, TCP/IP Filters, network based intrusion detection and Honey Pots. These tools can be used as well to protect the environment once a once a modem connection is authenticated. There is a need to track activity once the modem connection is authenticated because the authentication tools role is not enough protection. For example, when a ticket is issued for access to a film at the movie theater the film viewer generally has physical access to all of the theatres on location. In this same way, the remote user potentially has access to the rest of the server and potentially the rest of the network environment. For this reason, third party tools should be applied to protect the server to provide defense in depth.

On of the most common tools that can prevent malicious code from affecting the server is a firewall. When a firewall rule set is broken, the malicious activity is blocked and tracked in a log file that is written either locally or to a central management console. The three types of firewalls are named based on the way the firewall attempts to stop the malicious code. The three types of firewalls are packet filters, ingress filters, and egress filters. Packet filters are traditionally found on routers. These packet filters examine data at a fast pace but are easily fooled. On the other hand, an ingress filter, unlike that of a router side firewall, is an application firewall that is installed on a server. Ingress filters function to stop incoming packets by disassembles each packet as it is received and reassembles the packet for better perception of a threat from attacking the server such as a denial of service attack or a buffer overflow. The third type of filter is an egress filter. Egress filters can prevent hosts infected with a malicious program from sending packets that may be to numerous for the server to handle thus causing a server on the same network to shut down. Egress filters ability to detect and stop the malicious outbound code can stop traffic to a specific port such as the cancellation of the outbound connection through port 23. Ingress and egress filtering can be performed by routers, firewalls or anything else that ACKL's network traffic. When installed on a server a firewall can protect an organizations distributed environment from an attack by a remote user.

BlackICE Defender is an example of a commercially available firewall that works at the application layer with ingress and egress filtering. It’s designed to automatically

stop virus, worms, and Trojans just like a virus detection program. The firewall can also prevent and identify unauthorized connections to a host even from a modem or anywhere else on the network. BlackICE Defender creates highly detailed logs of the inbound connection such as source IP and packet type. Email alerts can be sent when high threat violations such as an unauthorized inbound connection attempts are made. These alerts and logs contain information which can be used to determine the source of the attack. Other firewall products on the market may be offered as free ware like Zone Alarm.

Zone Alarm was designed for Windows desktops as freeware firewall for academic institutions and commercial licensed version for corporations. Of course the commercial product offers greater functionality. For example, one feature in Zone Alarm Pro is the geographic maps of attack location attempts based on IP address. The commercial server product is the support for managing multiple servers cam be set with three general configurations of high, medium, and low security levels is easy. Pop-up windows can generate when a window for new access for a previously undefined network connection request is made. Programs that are allowed to access the internet automatically are benchmarked so no malicious software can be hidden in that code at a latter date such as any active content like ActiveX. Instead of commercial filter products like a Zone Alarm Pro and BlackICE firewall, there are possibilities when configuring the server to use other filters called TCP Filtering.

TCP/IP Filtering is free to implement because it works in Kernel of the Windows 2000 operating system to stop inbound and outbound connections. Servers in a workgroup or domain can all benefit from TCP/IP Filtering ability to manage unwanted connections. According to "HOW TO: Configure TCP/IP Filtering in Windows 2000", Q309798 "The way TCP/IP Filtering works is to verify new connections for TCP, UDP, and IP ports with those permitted or denied by the list of values." In this way, TCP/IP Filtering stops unwanted connections.

TCP/IP Filtering should be implemented to close any ports that threaten a server. The SQL Slammer Worm attacks servers on UDP port 1434. This worm was not stopped by virus protection software. This worm when in the wild can be stopped by TCP/IP Filtering to prevent buffer overflows of SQL servers by closing UDP port 1434 on the server. "By enabling filtering you can prevent many incoming connections while, at the same time, allowing outgoing and established connections to work normally," according to Anderson in his 2001 paper entitled "Basic Steps to Hardening a Standalone Windows 2000 Installation." Thus by stopping a connection to the server, TCP/IP Filtering can even prevent an attack and the spread of malicious code.

A draw back of TCP/IP Filtering is that it can only stop malicious in bound connection attempts that do not follow the TCP/IP Filter rule set. For example if no filters are in place malicious connection could continue to propagate. Another drawback of filtering connections is that they are not easily scalable for a large environment with numerous machines since each server would need to be setup individually. Otherwise, TCP/IP Filter technology can provide a low cost level of defense in depth that can stop attacks at the port level. Another way to track the use of TCP/IP ports and prevent the spread of malicious code is host based intrusion detection programs.

Host based intrusion detection programs alert system administrators of malicious activity. This detection technology works on quires, which require updates, just like the

traditional knowledge based check of virus and firewall protection technology. In this way, a host based intrusion detection system can detect the changes made to files and stop unapproved actions sent or received on all TCP UDP ICMP ports. The benefit of systems with host based intrusion detection technology is that real-time response to attacks while documenting results locally or at a central console. These programs can track, log and prevent activity that can occur before a standalone server or a networked computer is compromised. Once a remote user has authenticated to a server they may be able to threaten another host from the network if host based intrusion detection is not implemented. The QueSo utility can remotely determine the server's operating system based on the errors and other responses drawn from crafted TCP and UDP packets. There are commercially available tools like GFI LANguard Network Security Scanner which can be used to further threaten and detect open ports. Thus malicious activity can go unnoticed by perimeter firewall is an insider attack because the attack originates inside the firewall. Host based intrusion detection can stop attacks that may originate through a modem connection such as the spread of the SQL Slammer Worm to remote servers. The defense in depth strategy of host based intrusion detection programs protects remote connections made by the modem to other computers or from attacking the rest of the environment.

Intrusion detection technology was heightened in the 90's by Dr Gene Spafford when he and his colleagues at Purdue University released Tripwire to track the changes made to servers. "The basic function of Tripwire is to check the integrity of important files and directories against a baseline database and raise an alert when any changes occur within the preset policy" stated by Hrivnak in her 2002 paper titled "Host Based Intrusion Detection: An Overview of Tripwire and Intruder Alert." To better protect the files, a random salt bit is added to the file when encrypting to make the hash unique in size. The idea is that two similar files, when encrypted would not end up with the same end hash file result when the random extra value is combined to the encryption. This inconsistency in hash files would then alert system administrators to an unauthorized change to the source file. Even a change in a file that was moved between directories would create a different hash file than the original. When changes occur on those files designated to be monitored by Tripwire the program agents alert system administrators via email or event logs while changes are tracked. Also, a central management console can alert administrators that files have been changed without approval. The management console is connected via encrypted protocol SSL to allow easier, secure management of Tripwire protected files by the system administrator. The key here is to keep the hash or signature files that will be checked against a secure remote host. This is to prevent the vulnerability of a change to the hash file to match the new source file after an attack.

As published by Security Focus in the article titled "Tripwire Insecure Temporary File Symbolic Link Vulnerability" by Huuskonen in 2001, vulnerabilities in the "Tripwire manor of creating files may be insecure since the mktemp system calls do not check for an existing file since a local user can launch a symbolic link attack to overwrite system files, creating a denial of service, or potentially gain elevated privileges." Another drawback of Tripwire is the risk when file signatures are left on the same host that Tripwire is guarding. Since the signature on a compromised server could then be modified to remove traces of activity by a malicious user. This sort of change is similar

to the same reason an event log would get changed. Tripwire can be used as a successful third party strategy to track changes made to important files on there server that is connected to by remote third party users.

An example of a commercial grade host based intrusion detection system is Symantec Intruder Alert. This product supplies system administrators with a range of out of the box information for monitoring attacks. These rules can be customized to maintain the corporate baseline security standards. Intruder Alert agents' offer features like file integrity checkers which verifies that a file hasn't been changed without the system administrator's approval. Any unauthorized change activity of a hundred servers can report to a central server or desktop. The desktop has an administrator program installed that can hold information from the manager's agents that reside on each of the domains. Pushing new definition files out to a whole environment is possible from one workstation. This product allows for very easily managed defense.

There are of course drawbacks to the host based intrusion detection layer of defense. An example of this is a server that constantly has file changes will generate numerous false positive alerts. The value from intrusion detection is only after it has been configured on a stable server. It is not uncommon for system administrators to waste cycles to perfecting the initial implementation of these programs on a server based on the dynamics of their own environment. Other theorized weaknesses in host based intrusion detection programs demonstrate the need for network intrusion detection.

Network intrusion detection may be extreme for stand alone server that has a modem, but servers in a domain can threaten the rest of the environment. Researchers like Handley, Vern, and Kreibich have written in their 2001 paper entitled "Network Intrusion Detection: Evasion, Traffic normalization, and End-to-End Protocol Semantics." about "theorized attacks based on session splicing and packet fragmentation activity that may go unnoticed by host based intrusion detection." In their research custom TCP or UDP packets fragments are created from a tools like Hping to circumvent the host based intrusion detection filters so that the server reassembles the malicious code. These attacks obviously need to be researched further. According to Kamerling of the Sans Institute in his 2001 paper entitled "The Hping2 Idle Host Scan," stated "It (idle host scan) combines IP spoofing and network, or host scanning, into an effective way to perform an anonymous probe for services." This is an example of the type of an attack a remote attacker might perform on an organizations network. In this way, there is a need to monitor the packets that are sent between servers that are on a network that allows modems in the environment.

Network intrusion detection tools like Snort are designed to address these concerns with network attacks. The design of Snort was created by Martin Roesch and is based on Libpcaps which is a light weight rule set for network monitoring. This layer of defense is used for network intrusion detection, and this tool can illustrate the level of threat that these vulnerable modems are to servers and infrastructure by monitoring the traffic. This allows data packets that pass between the servers that reside on the IP network or modem line to be filtered for malicious packets. As described in "What is Snort?" by Caswell and Roesh in the 2003 article Snort "can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS

fingerprinting attempts, and much more." Alerts of malicious network packets can write to an event log or to a SQL database like MySql. System administrators then need only to query the event log for threats. This reporting capability is valuable because it can update desktops via Samba SMB client as a WinPopup message when a high level threat occurs. In their 2002 article "Snort," Search Systems states "Snort, which was the sole open source freeware product tested, clearly out-performed the proprietary products." To sum up, Snort is a free well established network detection tool that adds a level of defense in depth against attacks that may come from servers in a domain.

Deception is a unique concept for defending against remote attacks, or possible attacks from an organizations own environment. For example a server set up with a modem could mimic or mime a resource that is already in the environment for deceptive purposes. Deceptive programs such as Honey Pot technology have been devised to lure attackers into aiming their sights on machines that are not revenue generating but rather configured to mimic mannerisms of an insecure production server. The hope is that the host Honey Pot system has the same security vulnerabilities as real server and reaction times. Once attached the system administrator can then learn more about those attacking the server. Honey Pots and deception tool kit (DTK) created by Fred Cohen runs a notification on TCP port 365 and UDP port 365. So Fred's premise is that when an attacker Nmaps a machine the Nmap tool will report DTK on port 365. The attacker would then assume the server is a Honey Pot and move on to the next box, since the crown jewels would not be kept in a Honey Pot. This DTK deception feature is just like a car that has a sticker announcing a car alarm is present. The vehicle with a warning sticker may not be protected by an alarm but it can be perceived to be secure by way of deception.

Traditional deception technologies like Honey Pots are based on TCP Wrappers that control the interface by pooling deception content through a shared database in order to make modifications to source code of various UNIX operating systems. Microsoft's source code is not an open source and is made available to small privileged groups that are members of Microsoft's Government Security Program like Communist China. Thus for deception purposes in the Microsoft Windows environment deception through application modification is a more approachable path.

This is the approach that Maj. Donald P. Julian and his staff at the Computer Science Department at US Naval Post Graduate School took in their paper on deception technology for web based application deception. Their technique built a database of inputs that would slow output response times to a variety of malicious inputs that an attacker might use for buffer overflows of java server applet based websites. Thankfully enough their research group was deceived. The success of their research marks the need for more research in application based deception for the windows environment in order to build up the database of deception. Luckily third party products like Symantec Mantrap have begun to do just that. This third party tool incorporates detection and response technologies that mimic and deceive an attacker with responses to malicious commands. The caveat to having technology that realistically mimics malicious activity is that this miming resource could be used against the environment. It is wise to think twice before deception tools are introduced into the environment for they may become the weapons used against the environment. Though deception technology has demonstrated to be successful, some would say that security

through obscurity is not a good idea. Rather the better solution is to track the intrusions and changes made to the system.

Thus, there are numerous ways that malicious activity that originates from a modem connection to be logged and prevented in standalone or network environment. Like the film fan that is authenticated with the purchase of a movie ticket, the film fan and remote user must continue to be tracked once they have been allowed access to the physical venue. In this way, the computer industry has created tools like firewalls, TCP/IP Filters, host based intrusion detection systems, and network based detection systems and Honey Pots to stop authenticated users from violating the security of the computers. This cornucopia of tools can be combined for multiple layers of defense against the multiple risks that modems introduce in the environment.

Further tools attempt to manage both the authentication of the connection and track the actions of those connected to standalone or domain servers. Such tools are pcAnywhere, NetOp Remote Control, Citrix, and Virtual Private Networks. The following are ways these tools can be implemented to create a secure modem connection. These tools all provide a means for system administrators and vendors to connect securely to a production environment.

PcAnywhere is a remote connection tool that requires a server and client side application that works together to provide user authentication across modem connections. This tool allows for symmetric 128 bit encryption for remote connections that can cipher data that passes between hosts. There is a built in dial back feature that has the same weaknesses as when the modem it self initiates the user dial back. PcAnywhere users are authenticated to the system via the application prior to the user rights further validation with operating system logon screen. Connections to servers are based on IP or DNS name of the server. It is also possible to when "you don't specify an IP address to connect to, it (pcAnywhere) automatically scans your local subnet and displays any active listening hosts. Many do not know that if you place a 255 in place of the last octet, it will also scan and display listening hosts on remote subnets," according to Kris Kistler's May 2000 paper entitled "Paranoid PCAnywhere." Unfortunately, once while logging on to the console remote users can connect and attack other systems on the domain. According to the Security Focus article "pcAnywhere Denial of Service Vulnerability" Frankie Zie found weakness in pcAnywhere that "Under certain versions of pcAnywhere it is possible for remote clients to cause a denial of service attack against the pcAnywhere server. This is done by canceling a connection in the time period between when the status bar is displayed (pcAnywhere connecting...) and before the Login window appears." Also pcAnywhere licensing can be costly because every computer that an administrator desires to connect with pcAnywhere must have pcAnywhere installed and configured in the same manor for the connection to be completed.

In response to driving down the cost of remote access tools web based tools have been developed. One example is NetOp Remote Control tool that permits remote control of a host via a web browser. The data streams are encrypted with AES 256bit key while the authentication stream uses a combination of 256 bit AES, or 2048 bit Diffie-Hellman for dialing into a server or modem pool. Other connections can be restricted to those IP or MAC addresses that are part of the corporate infrastructure. In this way, no client software is required aside from a web browser. The session is fast,

seamless when hosted on an internal web server that is protected by the firewall. The authentication is based on host security settings such as Active Directory or a NetOp security server that manages the authentication. The NetOp Remote Control features a Chat option that allows for real time chat to the application vendor over the IP network. This could be useful for trouble shooting to ask why the new application is installed on the operating system drive. Of course, there is need for a whole paper to discuss the risks of new web based remote access tools like NetOp.

On the other hand there are tools that have a long history of secure remote access. Citrix technology was founded, in the late eighties by Edward Iacobucci, one of the lead engineers on IBM's OS/2 project. He saw the need for a user interface that could securely connect the distributed servers and clients he and IBM were creating. The need for secure remote access became Citrix MetaFrame which relied on the ICA Protocol. This technology further was licensed to Microsoft and branded as Terminal Services and the RDP Protocol.

Microsoft Terminal Server remote access technology uses a remote desktop protocol that has potential risks. According to an article titled "Microsoft Terminal Services vulnerable to MITM-attacks" authored by Forsberg in 2003, "information sent over the network is encrypted, there is no verification of the identity of the server when setting up the encryption keys for the session." This means that RDP is vulnerable to the previously discussed Man in the Middle attacks.

On the other hand, Citrix communication is confidential, integral, and available. Citrix MetaFrame has an encryption client known as independent computing architecture or ICA which works well over modems. The Citrix allows for the same secure functionality a system administrator would have while physically at a server, over a remote connection. An ICA remote connection will work even if the two operating systems are not compatible. This is possible because the ICA client sets separate from the graphical user interface from the program so that the Citrix host does all the work thus making the client a dumb-terminal. The gain of this technology is that no code, only user keystrokes, and screen updates get sent over the connections. For example from any desktop in the world, even at an airport that is shared by many airlines, an employee can install the ICA client, and connect to the corporate infrastructure without the risk of transferring malicious code back to the organizations network because the applications are not run on the local desktop.

Actually a desktop is not necessary; a PDA with a PCMCIA wireless Ethernet card, a network service provider and the 48mb free ICA client could remotely patch servers from the right field bleacher section at Wrigley Field at 1:20 in the afternoon. Citrix can go a step further with a product called Secure Gateway Server that when coupled with RSA Tokens make for a well authenticated secure tool for remote access. In this way, ICA can provide secure remote high speed connections for vendor support since no data is sent back and forth over a network. Citrix MetaFrame and Microsoft's Terminal service has began to offer products that have web base remote access and the ICA protocol has expanded to support virtual private networks.

Virtual private networks or VPN technology are designed for secure remote connectivity. This technology is based off IPSec but it relies on third party applications to create the network. The virtual private network is created between distributed clients across publicly switch telephone lines and authentication servers that seamlessly pass

the user rights to the production servers. The user's interaction across the remote connection is similar as to when the user is physically at part of the network. The security of the meta-network is based on authorized encrypted connections. This then lessons the risk to the organization via remote users from a potentially malicious telephone connection. The cryptography of the transmission ensures confidentiality of the communication access to the host. Unfortunately, the common criticism of encrypted networks is that this creates nothing more than secure hacking channels because the encrypted packets can't be read by a firewall or network intrusion detection program. Another caveat that still holds true with this form of remote user connection is that the risks of the remote connection that have been previously discussed are still potentially inherited across the network. Such risks like a Trojan and Virus can not be stopped by VPN but can be encrypted which offers no protection from this malicious code. This is not to say VPN technology should not be implemented. Aside from those threats VPN still offers better encryption, authentication, and seamless access to the whole network. VPN has proven to be a great step towards secure means of remote administration and a giant leap away from modem usage. This has contributed to the strong growth in product lines in the past few years that offer VPN.

Nortel Corporation offers VPN products with a client installation that is straight forward. In addition, the Microsoft Windows 2000 and XP VPN clients are free from Nortel. Nortel VPN servers perform a stateless fail over once a connection has been latent for to long so that users need to reconnect after a time out period. Authentication of the connection takes a matter of moments. Rights for users are just a directory tree. User groups are created and managed with an interface for the VPN administrators to work with. New users need each individual user account to manually get remote access rights for each individual device. This is time consuming to setup because if you have fifty users who need to connect to two hundred machines for remote system administrator duties than there are ten thousand connections that have to be set up! The next generation VPN products on the market today, like Nortel feature Web-based VPN, require no client software. The concept is dependent upon the use of internet browsers. Obviously the security risks of web based remote access tools need to be further pursued if VPN technology continues on this route.

The best solution for modem connectivity must provide a well authenticated, secure connection that can either limit or stop all malicious activity from instigating on the server or propagating through out the network. This can be achieved through the use of multiple layers of defense known as defense in depth. For example the server should have a firewall, TCP/IP Filtering, host based intrusion detection installed to protect against undesirable attacks or malevolent programs like Trojans. Authentication can be achieved with the creation and management of virtual private networks which are based off the IPSec protocol or through implementation of modem pools. Obviously, the auto answer function for all modems should be turned off and war dialing should be instigated as part of the organizations security policy. Further implementations of defense in depth may be necessary based on the organizations security needs.

In conclusion, it is important to eliminate the certainty of risk that a modem will introduce before the threat of an attack becomes a reality. For example, there is no risk of death to go for space walk without a space suit because an astronaut would die.

Undoubtedly, modems, like the unprotected space walk are bad choice. A production machine with a modem needs third party tools to protect, track, and authenticate connections from a modem. There are numerous answers and combination of solutions that reduce the vulnerabilities of modem connections. Thus, security needs to be implemented on the server to protect the server and networked environment from modem risks. These strategies need to reduce modem risk of poorly authenticated and insecure connections. Also, multiple means to track the activity that transpires from a remote connection to the server and the rest of the environment are necessary to protect the environment. There will always be a need in distributed client server environment for remote access, but this access needs to be secure and without a high level of risk. Successful security must provide redundant solutions to the risks modems present by limiting threat levels to an acceptable level or provide alternative actions to insecure technology like a modem.

List of References:

1) Academic Information Systems Columbia University. "Dial-Up Modem Pool." January 29, 2003. URL: http://www.columbia.edu/acis/access/offcampus/. (May 4, 2003).

2) Anderson, Todd. "Basic Steps to Hardening a Standalone Windows 2000 Installation." March 21, 2001. URL: http:rr.sans.org/index.php. (January 11, 2003).

3) Antirez. "Bugtraq: new tcp scan method." December 17, 1998. URL: http://lists.insecure.org/bugtraq/1998/Dec/0082.html. (May 6, 2003).

4) Ardoin, Lloyd V. "Nortel Instant Internet 100-s VPN Configuration." June 28, 2001. URL: http://rr.sans.org/index.php. (April 11, 2003).

5) AUBELIO. "GFiLANguard Network Security Scanner." Solutions communicantes pour les enterprises. 2003. URL: http://www.aubelio.com/lanscan.html. (April 11, 2003).

6) California State University. "Queso." K-12 Operating System Usage Survey. 2003. URL: http://econ.csuchico.edu/~harrison/k12linux/. (April 11, 2003).

7) Caswell, Brian, Roesh, Marty. "What is Snort?." January 28, 2003. URL: www.snort.org. (January 28, 2003).

8) Citrix Systems, Inc. "Citrix Independent Computing Architecture (ICA)." Citrix. 2003. URL: http://www.citrix.com/press/corpinfo/ica.asp. (February 22, 2003).

9) Cohen, Fred. "The Deception Toolkit Home Page and Mailing List." 2003. URL: http://www.all.net/dtk/dtk.html. (April 15, 2003).

10) CrossTec Corporation. "NetOp Remote for Windows." NetOp Remote Control. 2000. URL: http://www.crossteccorp.com/netopremote/index.html. (April 11, 2003).

11) Emery, David I. "Dialback Modem Security." File 8 of 12. April 7, 1988. URL: http://www.phrack.org/show.php?p=17&a=8. (April 24, 2003).

12) Equinox Systems. "Windows NT Modem Pooling Solution." 2002. URL: http://www.equinox.com/Typical_Deployment196.html. (May 5, 2003).

13) Forsberg, Erik. "Microsoft Terminal Services vulnerable to MITM-attacks." April 01, 2003. URL:

http://archives.neohapsis.com/archives/bugtraq/2003-04/0035.html. (April 10, 2003).

14) Handley, Mark Paxson, Vern and Kreibich, Christian. "Network Intrusion Detection: Evasion, Traffic normalization, and End-to-End Protocol Semantics." May 26, 2001. URL:http://www.icir.org/vern/papers/norm- usenix-sec-01.pdf. (January 28, 2003).

15) Hibbeln, David R. "Capturing an Analog Modem Transmission." March 21, 2002. URL: http://www.securityfocus.com/archive/105/263349. (April 24, 2003).

16) Hrivnak, Allison. "Host Based Intrusion Detection: An Overview of Tripwire and Intruder Alert." January 29, 2002. URL: http://rr.sans.org/index.php. (January 11, 2003).

17) Huuskonen, Jarno. "Tripwire Insecure Temporary File Symbolic Link Vulnerability." July 9, 2001. URL: http://www.securityfocus.com/bid/3003/discussion/. (January 23, 2003).

18) Insecure.org. "Nmap Stealth port scanner." February 22, 2003. URL: http://www.insecure.org/nmap/. (April 15, 2003).

19) Internet Security Systems. "BlackICE Server Protection." 2003. URL: http://blackice.iss.net/product_server_protection.php. (April 11, 2003).

20) Kamerling, Erik J. "The Hping2 Idle Host Scan." February 26, 2001. URL: http://www.sans.org/rr/audit/hping2.php. (April 26, 2003).

21) Kistler, Kris. "Paranoid PCAnywhere." May 29, 2000. URL: http://www.sans.org./rr/toppapers/paranoid.php. (May 6, 2003).

22) MAJ Juilan, Donald P; Rowe, Neil C.; Michael, J. Bret. "Experiments with Deceptive software Responses to Buffer-Based Attacks." URL: www.cs.nps.navy.mil/people/faculty/rowe/iajulian.htm. (March 10, 2003).

23) Microsoft Corporation. "HFNetChk." 2003 URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/hfnetchk.asp. (April 11, 2003).

24) Microsoft Corporation. "HOW TO: Configure TCP/IP Filtering in Windows 2000." Microsoft Knowledge Base Article: 309798." October 26, 2002. URL: http://support.microsoft.com/?kbid=309798. (April 25, 2003).

25) Microsoft Corporation. "Microsoft Baseline Security Analyzer." 2003. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP. (April 11, 2003).

26) Microsoft Corporation. “Microsoft and China Announce Government Security Program Agreement.” PressPass – Information for Journalists. February 28,2003. URL: http://www.microsoft.com/presspass/press/2003/Feb03/02-28GSPChinaPR.asp. (April 15, 2003).

27) Microsoft Corporation. “Microsoft Windows Update.” 2003 URL: http://v4.windowsupdate.microsoft.com/en/default.asp (April 11, 2003).

28) Microsoft Corporation. “Terminal Service.” Microsoft Windows 2000. URL: http://www.microsoft.com/windows2000/technologies/terminal/default.asp. (April 11, 2003).

29) Milroy, Derek. “Corp-Sec Practical Security for the Real World.” April, 04, 2003. URL. http://corp-sec.net/windows2khard.htm.l (March 30, 2003).

30) MySQL. “The World’s Most Popular Open Source Database.” 2003. URL: http://www.mysql.com/. (April 15, 2003).

31) One4net.com. “Raptor Firewall 6.5.” Products. 2003. URL: http://www.one4net.com/products/security/rapsec-cont.htm. (April 15, 2003).

32) Procheckup Security Bulletin PR01-02. “RAS SecurID Debug Mode Information Disclosure Vulnerability.” October 19, 2001. URL: http://www.securityfocus.com/bid/3462/discussion/. (January 23, 2003).

33) RSA Security INC. “3.6.1 What is Diffie-Hellman?.” 2003. URL: http://www.rsasecurity.com/rsalabs/faq/3-6-1.html. (June 3, 2003).

34) Sanfilipp, Salvatore. “DOWNLOAD HPING STABLE.” April 15, 2003. URL: http://www.hping.org/download.html. (April 15, 2003).

35) Sanstorm. “PhoneSweep – The Wardialer of Choice of Security Professionals” 2003. URL http://www.sandstorm.net/products/phonesweep/. (January 23, 2003).

36) Search System Management. “modem.” November 11, 2002. URL: http://searchsystemsmanagement.techtarget.com/sDefinition/0,,sid20_gci 212583,00.html. (March 30, 2003).

37) Search System Management. “Snort.” January 7, 2002. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci789029,00.ht ml. (April 15, 2003).

38) SecurityFocus. “ToneLoc 1.10.” Tools. 2003. URL:

http://www.securityfocus.com/tools/48. (April 11, 2003).

39) Security Writers Guild. “Honeynet@home.” 2002. URL: http://www.securitywriters.org/projects/honeynet/software.php. (January 23, 2003).

40) Shimonski, Robert. “Hacking techniques, War dialing.” August 2002. URL: http://www-106.ibm.com/developerworks/security/library/s-dial/. (January 29, 2003).

41) SourceForge. “Project: The libpcap project: Summary.” 2003. URL: http://sourceforge.net/projects/libpcap/. (April 16, 2003).

42) Symantec Corporation. “Symantec ManTrap.” Intrusion Detection. 2002 URL: http://enterprisesecurity.symantec.com/content/displaypdf.cfm?pdfid=292&EID=0. (April 15, 2003).

43) Symantec Enterprise Solutions. “Symantec Intruder Alert.” April 15, 2003. URL: http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=171&EID=0. (April 15, 2003).

44) TechTarget. “Port Scan.” 2003. URL: http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214054,00.html. (Janurary 24, 2003).

45) The SANS Institute. “How does attacker evade IDS with Session Splicing?” Intrusion Detection FAQ. 2003. URL http://www.sans.org/resources/idfaq/sess_splicing.php. (February 15, 2003).

46) The SANS Institute. “What is the role of a file integrity checker like Tripwire in intrusion detection?” Intrusion Detection FAQ. 2003. URL: http://www.sans.org/resources/idfaq/integrity_checker.php. (February 15, 2003).

47) Venema, Wietsa. “TCP Wrapper.” October 1994. URL: http://www.ccd.bnl.gov/pdsdir/pds/9410-tcp-wrapper.html. (April 11, 2003).

48) Wack, John. “Integrating Modem Pools with Firewalls.” Febuary 9, 1995. URL: http://csrc.nist.gov/publications/nistpubs/800-10/node59.html. (April 25, 2003).

49) Weber, Chris. “Using IPSec in Windows 2000 and XP, Part1.” December 5, 2001. URL: http://www.securityfocus.com/infocus/1519. (April 25, 2003).

50) Zarak. “TCP/IP over Dial-Up.” URL: http://www.zarak.com/new/index6.htm. (May 17, 2003).

51) Zie, Frankie. “PCAnywhere Denial of Service Vulnerability.” April 9, 2000. URL: http://www.securityfocus.com/bid/1095/discussion. (May 6, 2003).

52) Zone Labs, Inc. “Home And Small Business Solutions.” Smarter Security. April 11, 2003. URL: http://www.zonelabs.com/store/application?namespace=zls_main&origin=global.jsp&event=link.catalogHome&&zl_catalog_view_id=201&lid=nav_h o. (April, 11, 2003).

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event