Securing Your VoIP™

A CVE® WHITEPAPER

October 20, 2005

Gary S. Miliefsky, CISSP®

NetClarity
54 Middlesex Turnpike
Bedford, MA 01730-1417
781.276.4555 or 877-677-3328
www.netclarity.net

Contents

Introduction

The way we do business has changed dramatically since the advent of the Internet. Now, with new protocols for communication, enter the world of Voice over Internet Protocol (VoIP), which will forever change the way telephone calls are made.

Just look at the numerous offers for Vonage, a VoIP system designed to replace your standard telephone service by using the Internet to make local and long distance phone calls.

Or look at SKYPE, which is a software version of VoIP that rides your existing Internet connection to allow you to make calls to fellow SKYPE users anywhere in the world at no charge.

VoIP turns your analog audio signals into digital data that can be easily transmitted over the Internet. That's why there are millions of users of SKYPE making millions of Internet-based telephone calls daily, using their desktops or laptops, a microphone, headset, their built-in sound card, the Windows operating system, and the SKYPE peer to peer (P2P) software.

Your first question might be – how useful is VoIP? and your second question might be – is it safe? The answers to both questions are that yes, VoIP can be very useful and very inexpensive, but it also has a very high risk of being attacked, especially by eavesdropping and denial of service exploits – not good when you need to place an emergency phone call or when you are giving your credit card information out to make a purchase using your VoIP telephone.

Let's take a look at how VoIP works.

How VoIP Works

When you want to place a call using VoIP, you can do it in one of three different ways:

- ►Through an Analog Telephone Adaptor
- ►Through an IP (Internet Protocol) Telephone
- ►Through Peer to Peer VoIP

The first and easiest way to make a VoIP call is through an ATA (Analog Telephone Adaptor), which are sometimes called "Gateways." These ATAs let you use your existing 'old fashioned' analog telephone. All you have to do is plug your antiquated handset into the ATA and then connect the ATA to your Internet Connection (Cable modem or sometimes directly into your computer) and you are ready to place calls.

A Gateway takes the analog signal from your dusty old phone and turns the sound waves into digital signals that can be easily transmitted over the Internet. Some of the Gateways come with additional software that is loaded onto your personal computer, enabling you to configure it for VoIP and monitor VoIP status.

Another way to do VoIP is to use an IP (Internet Protocol) telephone. These telephone handsets look just like normal handsets, however, they have an RJ45 Ethernet connector instead of the standard RJ11 connector. These phones are just like "micro" computers and have all the software and hardware built-in to them to get an IP address to be online for making and receiving telephone calls. Because they connect directly to your Internet connection, they are very fast to setup, install and use, just like an old fashioned telephone.

Finally, as we've seen with Peer to Peer (P2P) systems like SKYPE, you can do computer to computer VoIP. All you have to do is install the software, configure it properly and begin using your microphone and headset attached to your PC. SKYPE promises to be 'free forever' and other services are coming online that will offer the same price – not bad. So what is the catch? You might want a VoIP call to be forwarded to your cell phone when you are away from your computer or might want voice mail and other features – these "options" are not free, so there's the catch. The more options you want, such as Caller ID, Voice Mail, Inbound Fax, Call Forwarding, Call Waiting, etc., the more you will pay for systems like SKYPE.

Computer to computer – This is the easiest way to make use of the VoIP technology. There are many companies offering cost effective software that you can use for this type of VoIP. Usually the only charge you pay is the monthly one from your Internet service provider, even for long distance calls. All you need is a microphone, speakers, a suitable sound card, and a fast Internet connection.

There's a high probability that you've already made a VoIP call without even realizing it. Maybe you've called your local bank and the branch manager who answered the phone was on a VoIP telephone. Most major telephone carriers are already using VoIP to route

thousands of long distance calls through a circuit switch and into an Internet Protocol (IP) Gateway.

Your call is received by a remote IP Gateway at the other end and then routed into a local circuit switch on the other side. As more companies install VoIP phone systems, the technology will grow and reach a disruptive state, becoming a commodity, available everywhere – this is happening as you read this document. Disruptive and powerful new technologies usually catch on like wildfire. VoIP is one of them.

VoIP Features

One of the best features of VoIP is portability—can you take your old fashion home telephone into your doctors' office waiting room or your accountants' office and make a telephone call from your phone number? Nope. But with VoIP, you can make calls from anywhere that you can plug into an Internet jack (RJ45 connection) and make calls as if you were home. If your VoIP rings, someone has dialed your local VoIP telephone number, even if it is ringing from your hotel room in Hawaii—now that's really cool technology.

If you are using a soft-phone (VoIP software such as SKYPE), then you can make and receive calls wherever you run this software—if it is on your laptop, then your phone number is now Mobile—wherever you have access to the Internet, including a coffee shop or the airport, your telephone is moving with you.

Most old-fashioned telephone carriers charge you for all those extra features you love but with VoIP accounts they usually come standard, unless you are using a free soft-phone like SKYPE. These are the kinds of standard features you can have access to with your VoIP telephone service:

Standard Features of VoIP Phone

1. Call Waiting
2. Caller ID
3. Call Transfer
4. Repeat Dialing
5. Return Last Call
6. Three-Way Dialing

There are even additional features available from some VoIP service providers. These additional features allow you to decide how calls to a specific number can be automatically handled or "filtered" by using Caller Identification (ID). They include:

Special Filtering Features of VoIP

1. Send the call directly to voicemail
2. Forward the call to a particular number
3. Give the caller a busy signal
4. Play a "not-in-service" message

With most VoIP services, you can check your voice mail over the internet or have it sent to you as an email attachment that you can play as a sound file (like you would play in Windows Media Player).

VoIP Benefits

There are many cost saving benefits that arise from flattening out your network architecture – for example, your phone system and your internet access can all come from the same network and service provider.

If you are Network Administrator or Information Technology (IT) Professional, this technology holds the potential of a streamlined communication system – instead of managing two networks (the telephone system) and the Internet/intranet, you can manage one network.

The portability of VoIP systems is excellent for improving communications and ease of access to sales staff, partners, customers, and fellow VoIP users. If you are the Network Administrator and you need to make changes to voice mail for new hires, it can be done right over the Internet/intranet using a web browser with simple point and click software.

If you have many branch offices, you might want to flatten out how your corporation appears – a call made far away to a branch in California can be routed to a branch in New York without the caller even knowing this routing took place. You can benefit from a flatter, easier communication environment with:

1. One receptionist for all calls
2. Auto attendant features for all calls
3. Corporate-wide Voice Mail managed from one location
4. Updates to the phone system executed across the entire organization at once

Choosing a VoIP System

If you have decided that a VoIP phone system is the right move for your company, next you need to determine how much of your existing telephone equipment you are able to keep. The potential cost savings associated with retaining any existing digital equipment are huge. Many digital phone systems can be IP enabled using minor hardware additions and software upgrades.

When shopping around for potential systems you need to be certain of the features each VoIP supplier provides as standard and the features that are optional cost extras.

You also need to be certain of exactly what is included with the system. Many suppliers claim to include everything you need, but standard components can vary from one company to the other. So you need to sure you are comparing equivalent systems when approaching potential suppliers.

You will also need to:

- Inquire about the compatibility of existing equipment. The technology used in many VoIP systems may affect the implementation of any existing telephone hardware.
- Ensure that any existing devices, such as fax machines, credit card processors, security systems, and the like, can be integrated into your new VoIP phone system. Make any potential vendor aware of such devices so they can provide you with a suitable phone system for your requirements.

A note of caution: Do not try to save money by buying used VoIP phone systems. Remember VoIP is a new technology, so even last year's equipment is outdated. Also the installation cost will still apply whether the system is new or second hand, and the service costs with a used VoIP may even be higher due to reliability issues. Used VoIP systems just aren't worth the hassle. The higher secondary costs will wipe out any potential saving.

The next section details some of the potential threats and vulnerabilities in a VoIP environment, including vulnerabilities of both VoIP phones and switches.

VoIP Security Flaws

This discussion is included because the variety of threats faced by an organization determines the priorities in securing its communications equipment. Not all threats are present in all organizations. A commercial firm may be concerned primarily with toll fraud, while a government agency may need to prevent disclosure of sensitive information because of privacy or national security concerns.

Information security risks can be broadly categorized into the following three types:

- Confidentiality
- Integrity
- Availability

You can remember these categories with the mnemonic "CIA".

Additional risks relevant to switches are:

- Fraud
- Risk of physical damage to the switch, physical network, or telephone extensions.

Packet networks depend for their successful operation on a large number of configurable parameters: IP and MAC (physical) addresses of voice terminals, addresses of routers and firewalls, and VoIP specific software such as Call Managers and other programs used to place and route calls. Many of these network parameters are established dynamically every time a network component is restarted, or when a VoIP telephone is restarted or added to the network. Because there are so many places in a network with dynamically configurable parameters, intruders have a wide array of potentially vulnerable points to attack.

Vulnerabilities described in this article are generic and may not apply to all systems; however, investigations by NIST and other organizations have found these vulnerabilities in a number of VoIP systems. This list is not exhaustive; as systems may have security weaknesses that are not included in the list. With each potential vulnerability mentioned there are some recommended actions to eliminate or reduce the risk of compromise.

Confidentiality and Privacy

Confidentiality refers to the need to keep information secure and private. For home computer users, this category includes confidential memoranda, financial information, and security information such as passwords.

In a telecommunications switch, the risk of intruders eavesdropping on conversations is an obvious concern, but the confidentiality of other information on the switch must be protected to defend against toll fraud, voice and data interception, and denial of service attacks. Network IP addresses, operating system type, telephone extension to IP address mappings, and communication protocols are all examples of information that, while not critical as individual pieces of data, can make an attacker's job easier.

With conventional telephone systems, eavesdropping usually requires either physical access to tap a line or penetration of a switch. Attempting physical access increases the intruder's risk of being discovered, and conventional PBXs have fewer points of access than VoIP systems. With VoIP, opportunities for eavesdroppers increase dramatically, because of the many nodes in a packet network.

Switch Default Password Vulnerability

It is common for switches to have a default login/password set, such as admin/admin, or root /root. If no one changes this default, it becomes a vulnerability that allows wiretapping of conversations on the network with port mirroring or bridging. Once an attacker has access to the switch administrative interface, the attacker can mirror all packets on one port to another, allowing the indirect and unnoticeable interception of all communications.

Preventing use of this vulnerability may seem straightforward, but failing to change default passwords is one of the most common errors made by inexperienced users. Another way to close this vulnerability is to, if possible, disable remote access to the graphical user interface to prevent the interception of plain text administration sessions. Some devices provide the option of a direct USB connection in addition to remote access through a web browser interface, another accessway you can close. You should also consider disabling port mirroring on the switch.

Classical Wiretap Vulnerability

Attaching a packet capture tool or protocol analyzer to the VoIP network segment makes it easy to intercept voice traffic.

How can you prevent such interception? A good physical security policy for the deployment environment is a general first step to maintaining confidentiality. Disabling the hubs on IP Phones as well as developing an alarm system for notifying the administrator when an IP Phone has been disconnected will allow for the possible detection of this kind of attack.

ARP Cache Poisoning and ARP Floods

Because many systems have little authentication, an intruder may be able to log on to a computer on the VoIP network segment, and then send ARP commands corrupting ARP caches on sender(s) of desired traffic. The intruder can then activate IP. An ARP flood attack on the switch could render the network vulnerable to conversation eavesdropping. The act of broadcasting ARP replies blind is sufficient to corrupt many ARP caches.

By corrupting the ARP cache, the attacker can now re-route traffic to intercept voice and data traffic.

To prevent this type of attack, use authentication mechanisms provided wherever possible and limit physical access to the VoIP network segment.

Web Server Interfaces

Both VoIP switches and voice terminals are likely to have a web server interface for remote or local administration. An attacker may be able to sniff plain text HTTP packets to gain confidential information. This action would require access to the local network on which the server resides.

To prevent such an attack, if possible, do not use an HTTP server. If it is necessary to use a web server for remote administration, use the more secure HTTPS (HTTP over SSL or TLS) protocol.

IP Phone Netmask Vulnerability

An effect similar to the ARP Cache Vulnerability can be achieved by an attacker assigning a subnet mask and router address to the phone. The attacker crafts those addresses so that most or all of the packets the phone transmits will be sent to the attacker's MAC address. Again, standard (1q aware) IP forwarding makes the intrusion all but undetectable.

Setting up a firewall filtering mechanism can reduce the probability of this attack. Remote access to IP phones is a severe risk.

Extension to IP Address Mapping Vulnerability

An intruder can readily discover the IP address that corresponds to any extension. All it requires is calling that extension and getting an answer. A protocol analyzer or packet capture tool attached to the hub on the dialing instrument will see packets directly from the target instrument once the call is answered.

Being able to find out the IP address of a particular extension is not a compromise in itself, but makes it easier to execute other attacks. For example, if the attacker is able to sniff packets on the local network used by the switch, it will be easy to pick out packets sent and received by a target phone. Without knowledge of the IP address of the target phone, the attacker's goal may be much more difficult to reach and require much more time, possibly enough time that the attack could be foiled.

While disabling the hub on the IP Phone will prevent this kind of attack, it is a rather simple task to turn the hub back on.

Integrity Issues

Integrity of information means that information remains unaltered by unauthorized users. For example, most users want to ensure that bank account numbers cannot be changed by anyone else, or that passwords are changed only by the user or an authorized security administrator. Telecommunication switches must protect the integrity of their system data and configuration. The richness of feature sets available on switches provides an attacker with plenty of tools. A hacker who can compromise the system configuration has opened the door to a variety of potential hacks. For example, a hacker could reassign an ordinary extension into a pool of phones that the hacker can then eavesdrop on the same way that supervisors can legitimately listen in on or record conversations for quality control purposes.

Another action the intruder can take is to damage or delete information about the IP network used by a VoIP switch, producing an immediate denial of service.

The security system itself provides capabilities for system abuse and misuse. Compromise of the security system not only allows system abuse but also allows the abuser to eliminate all traceability,(covering his tracks) and insert trapdoors for future intruders to use on their next visit. For this reason, the security system must be carefully protected.

Integrity threats include techniques that can result in system functions or data being corrupted, either accidentally or as a result of malicious actions. Misuse is not restricted to outsiders, and may often involve legitimate users (insiders performing unauthorized operations) as well as outside intruders.

A legitimate user may perform an operations function incorrectly, or take unauthorized action, resulting in deleterious modification, destruction, deletion, or disclosure of switch software and data. This threat may be opened up by several factors, including the possibility that the level of access permission granted to the user is higher than what the user needs to remain functional.

Intrusion

There are a number of serious intrusion threats the intruder may carry out. By masquerading as a legitimate user, an intruder may access an operations port of the switch. Or the intruder may use the permission level of the legitimate user and perform damaging operations functions such as:

- Disclosing confidential data
- Causing service deterioration by modifying the switch software
- Crashing the switch
- Removing all traces of the intrusion by modifying the security log

Insecure State

At certain times the switch may be vulnerable due to the fact that it is not in a secure state. For example:

After a system restart, the old security features may have been reset to insecure settings, and new features may not yet be activated. (For example, all old passwords may have reverted to the default system-password, because new passwords are not yet assigned.) The same may happen at the time of a disaster recovery.

At the time of installation the switch may be vulnerable until the default security features have been replaced.

DHCP Server Insertion Attack

It is often possible to change the configuration of a target phone by exploiting the DHCP response race when the IP phone boots. As soon as the IP phone requests a DHCP response, a rogue DHCP server can initiate a response with data fields containing false information.

This attack allows for possible man in the middle attacks on the IP-media gateway and on IP Phones. Many methods exist that give the hacker the potential to reboot the phone remotely, for instance, utilizing "social engineering", ping flood, MAC spoofing (probably SNMP hooks and the like).

A preventive strategy would be, if possible, to use static IP addresses for the IP Phones. This implementation will negate the necessity of using a DHCP server. Further, using a state based intrusion detection system can filter out DHCP server packets from unauthorized IP Phone ports, allowing this traffic only from the legitimate server.

TFTP Server Insertion Attack

It is possible for a hacker to change the configuration of a target phone by exploiting the Trivial File Transfer Protocol (TFTP) response race when the IP phone is resetting. A rogue TFTP server can supply spurious information before the legitimate server is able to respond to a request. This attack allows an attacker to change the configuration of an IP Phone. Using a state based intrusion detection system can filter out DHCP server packets from IP Phone ports, allowing such traffic only from the legitimate server. Organizations looking to deploy VoIP systems should look for IP Phone instruments that can download signed binary files.

Availability and Denial of Service

Availability refers to the notion that information and services will be available for use when needed. Availability is the most obvious risk for a switch.

Attacks exploiting vulnerabilities in the switch software or protocols may lead to deterioration in service or even denial of service or denial of some functionality of the switch. For example: if unauthorized access can be established to any branch of the communication channel (such as a CCS link or a TCP/IP link), it may be possible to flood the link with bogus messages, causing severe deterioration (possibly denial) of service. A voice over IP system may have even more vulnerabilities when it is connected to the Internet. Because intrusion detection systems (IDS) fail to intercept a significant percentage of Internet based attacks, once attackers circumvent the IDS, they may be able to bring down VoIP systems by exploiting weaknesses in Internet protocols and services.

Any network can be made vulnerable to denial of service attacks simply by overloading the capacity of the system. With VoIP the problem may be especially severe, because of its sensitivity to packet loss or delay.

CPU Resource Consumption Attack without any account information

An attacker with remote terminal access to the server may be able to force a system restart (shutdown all/restart all) by providing the maximum number of characters for the login and password buffers multiple times in succession. Additionally, IP Phones may reboot as a result of this attack.

In addition to producing a system outage, the restart may not restore uncommitted changes or, in some cases, may restore default passwords, introducing the possibility of intrusion vulnerabilities. The deployment of a firewall disallowing connections from unnecessary or unknown network entities is the first step to overcoming this problem. However, there is still the opportunity for an attacker to spoof his MAC and IP address, circumventing the firewall protection.

Default Password Vulnerability

Just as switches have a default login/password sets, VoIP telephones often have default keypad sequences

that can be used to unlock and modify network information.

This vulnerability opens up the prospect of an attacker taking control of thenetwork topology remotely, allowing for not only complete denial of service to the network, but also for a port mirroring attack to the attacker's location. The mirroring attack would give a hacker the ability to intercept any other conversations taking place over the same switch. Further, the switch may have a web server interface that the hacker can use to disrupt the network without advance knowledge of switch operations and commands.

In most systems, telephones download their configuration data on startup using TFTP or similar protocols. The configuration specifies the IP addresses for Call Manager nodes, so an intruder could substitute a different IP address pointing to another call manager that would allow eavesdropping or traffic analysis. This kind of potential for intrusion means changing the default password is crucial. And disabling the graphical user interface is also required to prevent the interception of plain text administration sessions.

Exploitable Software Flaws

Like other types of software, VoIP systems have been found to have vulnerabilities due to buffer overflows and improper packet header handling. These flaws typically occur because the software is not validating critical information properly. For example, a short integer may be used as a table index without checking whether the parameter passed to the function exceeds 32,767, resulting in invalid memory accesses or crashing of the system.

Exploitable software flaws typically result in two types of vulnerabilities:

- Denial of service
- Revelation of critical system parameters

An intruder can implement a Denial of Service remotely, by passing packets with specially constructed headers that cause the software to fail. The goal is to get the system to crash, producing a memory dump that the intruder can search to find IP addresses of critical system nodes, passwords, or other security-relevant information. In addition, buffer overflows that an intruder can use to introduce malicious code exist in VoIP software, just as they exist in other applications.

These problems require action from the software vendor and distribution of patches to administrators.

Clever intruders are on top of the issues; they monitor announcements of vulnerabilities, knowing that many organizations will require days or weeks to update their software. Being sure your organization regularly checks for software updates and patches is essential to reducing these vulnerabilities.

Automated patch management can assist in reducing the window of opportunity for intruders to exploit a known software vulnerability. This window of time during which organizations are vulnerable is also known as the "vulnerability gap"—a gap all organizations can close by being up-to-date on patches, usually using automated systems.

Account Lockout Vulnerability

An account lockout vulnerability is a situation where an attacker can attempt to access an account several times using an incorrect login at the telnet prompt until the account becomes locked out.

Once the account is locked out, no one may connect to the machine for the set lockout time period. The effect is a denial of service. Because this problem takes advantage of a feature common to most password-protected systems (as part of trying to prevent attackers from making repeated login attempts until the correct password is found), it is difficult to circumvent. If such an attack occurs and if remote access is not available to legitimate users as a result, this problem can be solved with physical access control.

Securing Your VoIP

Properly securing your Voice over IP system is a complex process because VoIP is the integration of data and voice into a single network. Your network may be subject to daily attacks by hackers, viruses, and worms. With your old fashion phone system you you would never consider worrying about these types of attacks taking place.

There are nine steps that the National Institute for Standards (NIST) recommends you take to secure your VoIP network:

1. Develop appropriate network architecture for voice and data communications.

2. Examine the risk around deploying VoIP for voice communications.
3. Take special precautions for ensuring Emergency 911 (E-911) services.
4. Deploy physical controls are especially important in VoIP security.
5. Consider additional power backup requirements to ensure continued VoIP availability during power outages
6. Find, evaluate, and deploy VoIP-ready firewalls.
7. Avoid using 'softphone' solutions, as they are harder to manage and secure.
8. If mobile devices are part of your VoIP deployment, make sure they are secured using WPA and not WEP.
9. Review regulatory requirements regarding privacy and record retention.

Develop Appropriate Network Architecture

Separate voice systems from data systems by putting each on a logically different network if feasible. Different subnets with separate RFC 1918 address blocks for voice and data traffic and with separate DHCP servers for each will ease incorporation of intrusion detection and VoIP firewall protection.

At the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or other VoIP protocols from the data network.

Use strong authentication and access control on the voice gateway system, as with any other critical network component. Strong authentication of clients towards a gateway often presents difficulties, particularly in key management. Here, access control mechanisms and policy enforcement may help.

A mechanism to allow VoIP traffic through firewalls is required. There are a variety of protocol dependent and independent solutions, including application level gateways (ALGs) for VoIP protocols, Session Border Controllers, or other standards-based solutions when they mature.

Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. (This may not be practical when multimedia protocol inherent security or lower layer security is applied; for example, H.235 Annex D for integrity provision or TLS to protect SIP signaling.)

Use IPsec or Secure Shell (SSH) for all remote management and auditing access. If practical, avoid using remote management at all and do IP PBX access from a physically secure system.

If performance is a problem, use encryption at the router or other gateway, not the individual endpoints, to provide for IPsec tunneling. Since some VoIP endpoints are not computationally powerful enough to perform encryption, placing this burden at a central point ensures all VoIP traffic emanating from the enterprise network has been encrypted. Newer IP phones are able to provide Advanced Encryption System (AES) encryption at reasonable cost.

Note that Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.

Examine the Risk Around Deploying VoIP

It is important that you examine the issues with deploying VoIP to ensure that the organization can acceptably manage and mitigate the risks to information, system operations, and continuity of essential operations when deploying VoIP systems.

An especially challenging security environment is created when new technologies are deployed. Risks often are not fully understood, administrators are not yet experienced with the new technology, and security controls and policies must be updated. Therefore, organizations should carefully consider such issues as their level of knowledge and training in the technology; the maturity and quality of their security practices, controls, policies, and architectures; and their understanding of the associated security risks.

VoIP can provide more flexible service at lower cost, but there are significant tradeoffs that must be considered. You can expect VoIP systems to be more vulnerable than conventional telephone systems, in part because they are tied in to the data network, resulting in additional security weaknesses and avenues of attack. Confidentiality and privacy may be at increased risk in VoIP systems unless strong controls are implemented and maintained. An additional concern is the relative

instability of VoIP technology compared with established telephony systems. Today, VoIP systems are still maturing and dominant standards have not emerged. This instability is compounded by VoIP's reliance on packet networks as a transport medium. The public switched telephone network is ultra-reliable. Internet service is generally much less reliable, and VoIP cannot function without Internet connections, except in the case of large corporate or other users who may operate a private network. Essential telephone services, unless carefully planned, deployed, and maintained, will be at greater risk if based on VoIP.

Special Considerations for 911 Services

Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.

Unlike traditional telephone connections that are tied to a physical location, VoIP's packet switched technology allows a particular phone number to be anywhere. This is convenient for users, because calls can be automatically forwarded to their locations. But the tradeoff is that this flexibility severely complicates the provision of E-911 service, which normally provides the caller's location to the 911 dispatch office. Although most VoIP vendors have workable solutions for E-911 service, government regulators and vendors are still working out standards and procedures for 911 services in a VoIP environment. Organizations must carefully evaluate E-911 issues in planning for VoIP deployment.

Physical Security for the VoIP System

Organizations should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially connect network monitoring tools and tap into telephone conversations. Although conventional telephone lines can also be monitored when physical access is obtained, in most offices with a VoIP many more points exist where anyone can connect to a LAN without arousing suspicion. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis and determine the parties that are communicating. You should, therefore, ensure that adequate physical security is in place to restrict access to VoIP network components.

Physical securities measures, including barriers, locks, access control systems, and guards, are the first line of defense for the VoIP system. Organizations must make sure that these physical countermeasures are in place to mitigate some of the biggest risks such as insertion of sniffers or other network monitoring devices. Otherwise, practically speaking, this means that installation of a sniffer could result in not only data being accessed, but all voice communications being intercepted.

Costs for Additional Backup Systems

Evaluate costs for additional power backup systems that may be required to ensure continued operation during power outages. Conduct a careful assessment to ensure that sufficient backup power is available for the office VoIP switch, as well as each desktop instrument. Costs may include electrical power to maintain UPS battery charge, periodic maintenance costs for backup power generation systems, and cost of UPS battery replacement. If emergency/backup power is required for more than a few hours, electrical generators will be required. Costs for these include fuel, fuel storage facilities, and cost of fuel disposal at end of storage life.

VoIP-Ready Firewalls and VoIP Security Features

VoIP-ready firewalls and other appropriate protection mechanisms should be deployed. Organizations must enable, use, and routinely test the security features included in VoIP systems.

Because of the inherent vulnerabilities (such as susceptibility to packet sniffing) when operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. Organization security policy should ensure that these features are used. Additional measures, described in this document, should be added. In particular, firewalls designed for VoIP protocols are an essential component of a secure VoIP system.

Restriction of Softphone Systems

If practical, "softphone" systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern, because worms, viruses, and other malicious software are extraordinarily common on PCs connected to the Internet, and very difficult to defend against. Well-known vulnerabilities in web browsers make it possible for attackers to download malicious software without a user's knowledge, even if the user does nothing more than visit a compromised web site.

Malicious software attached to email messages can also be installed without the user's knowledge, in some cases even if the user does not open the attachment. These vulnerabilities result in unacceptably high risks in the use of "softphones," for most VoIP site installations. In addition, because PCs are on the data network, a softphone system conflicts with the need to separate voice and data networks to the greatest extent practical.

Protection of Mobile Systems on the VoIP System

If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).

The security features of 802.11 WEP provide little or no protection because WEP can be cracked with publicly available software. The more recent WiFi Protected Access (WPA), a snapshot of the ongoing 802.11i standard, offers significant improvements in security, and can aid integrating wireless technology with VoIP systems.

NIST strongly recommends that the WPA (or WEP if WPA is unavailable) security features be used as part of an overall defense-in-depth strategy. Despite their weaknesses, the 802.11 security mechanisms can provide a degree of protection against unauthorized disclosure, unauthorized network access, or other active probing attacks. However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for Federal agencies that have determined certain information must be protected via cryptographic means. As currently defined, neither WEP nor WPA meets the FIPS 140-2 standard. In these cases, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport Level Security (TLS), or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect information, regardless of whether the nonvalidated data link security protocols are used.

Compliance with Privacy/Record Retention Statutes

Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

Although legal issues regarding VoIP are beyond the scope of this document, readers should be aware that laws and rulings governing interception or monitoring of VoIP lines, and retention of call records, may be different from those for conventional telephone systems. Organizations should review these issues with their legal advisors.

The Magnitude of VoIP Vulnerabilities

Everyone knows that VoIP has been experiencing rapid growth. Even still, you might be surprised to learn that:

- 10% of all voice traffic is now transmitted with VoIP technology (IDC)
- AT&T will have VoIP service available to the top 100 US markets by the end of the first quarter 2004 (AT&T)
- It is estimated that 7 million IP Phones will be in circulation by 2007 (InStat/MDR)

The mass deployment of this new technology brings along with it many challenges—one area the security of your network.

"Because IP networks are subject to sophisticated, automated attacks, voice traffic on those networks is more vulnerable" says David Fraley, author of "Cyberwarfare: VoIP and Convergence Increase Vulnerability".

In fact, the UK's National Infrastructure Coordination Centre (NICC) has released findings that equipment from many vendors who have implemented the H.323 protocol standard for IP Telephony contains flaws attackers can exploit. (for more detail, visit http://www.uniras.gov.uk/vuls/2004/006489/h323.htm)

According to tests commissioned by NICC, these vulnerabilities can leave products open to:

- Denial-of-Service (DoS) attacks
- Buffer-overflow attacks
- Insertion of malicious code into the compromised equipment

According to CERT Advisory Number CA-2004-01 (visit the http://www.cert.org/advisories/CA-2004-01.html location), companies affected by these vulnerabilities include:

Cisco	Stonesoft
Check Point	WatchGuard
NetScreen	3COM
Nokia	AT&T
Microsoft	D-Link
Nortel	Extreme
Avaya	Foundry
Alcatel	Fujitsu
F5	Hitachi
Secure Computing	Intel
Cyberguard	Juniper
Symantec	NEC

As just one example, Cisco alone has many products that contain vulnerabilities in processing H.323 messages.

All Cisco products that run Cisco IOS software and support H.323 packet processing (http://www.cisco.com/warp/public/707/cisco-sa-20040113-h323.shtml#process):

- IOS Firewall
- IOS Network Address Translation
- Call Manager
- Conference Connection
- 7905 IP Phone
- BTS 10200 Softswitch
- Internet Service Node
- H.323 Gateway, H.323 Gatekeeper
- ATA18x Series Analog Telephony Devices

In some cases, Cisco does not plan to fix the vulnerabilities that have been identified.

To help you deal with VoIP's inherently vulnerable nature, you should be aware that there are a number of possible attacks that can be more readily perpetrated against a VoIP than against a standard network. The next section presents some of those attacks.

Possible VoIP Attacks

You should be alert to the types of attacks on your VoIP that CVEs can make it vulnerable to, including:

- Man in the Middle (eavesdropping and altering)
- Denial of Service (DoS)
- Compromise of Gateways
- Compromise of Endpoints — Impersonation

QoS and Security Issues

Quality of Service (QoS) refers to the speed and clarity expected of a VoIP conversation. QoS attacks are easier to pull off than other attacks, without a hacker going to extremes—no longer is it necessary for a hacker to "take down" an entire network; the hacker can merely "slow down" traffic.

QoS attacks are hard to defend against: Implementing proper security measures such as firewalls and encryption still leaves your VoIP vulnerable to latency and jitter.

Latency

Latency is the time from when words are spoken until they are heard at the other end. Latency greater than 150 milliseconds is unacceptable in most cases.

Jitter

Jitter is a series of non-uniform delays. Jitter requires buffering at the endpoints and application level reordering, which produces more latency. Increased jitter makes it hard to tell when a packet is missing or just late.

Packet Loss

VoIP is highly sensitive to packet loss. Loss Rates as low as 1% can garble communications.

Latency and Jitter can contribute to "virtual packet loss" as packets arriving after their deadline are as good as "lost."

Firewalls, NAT Routers, and Encryption

The Old Stand-By's are not as reliable as they used to be: Firewalls, Network Address Translation (NAT) routers, and encryption suffer from these shortcomings:

- Cannot be Implemented in a VoIP network without special considerations—standard components are not built for VoIP's high rate / small packet traffic pattern.
- They degrade the Quality of Service (QoS) by causing Latency, Jitter, and Packet Loss.
- They obstruct the call set up process by blocking incoming calls.

Firewalls

Firewalls filter out malicious traffic based on a set of rules and are needed to protect networks from outside attacks. They also secure the internal barrier between voice and data networks.

Firewalls and QoS

Firewall traffic investigation adds latency to the system and heavy data traffic can introduce jitter, which reduces the quality of service (QoS).

To resolve this issue, implement firewalls with fast CPU's to handle the high rate of packet delivery. Use QoS-aware firewalls.

IPSec

In ESP Tunnel Mode, IPSec protects both the data and the identities of the endpoints. IPSec is the standard encryption suite for the Internet Protocol and will be fully supported in IPv6.

Problems with IPSec include:

- Encryption can be used to secure voice data and avoid the firewall problems.
- Encryption introduces latency/jitter
- Encryption/decryption process takes time
- Crypto-engine schedulers do not implement QoS

Solutions include packet compression schemes, which have experimentally aided performance. QoS-aware scheduling before and after encryption heuristically improves performance.

Network Address Translation (NAT)

Network Address Translation (NAT) is used to allow multiple terminals to share a single IP address. It allows security measures to be consolidated at the NAT router and hides information about the structure of the internal network.

The problem with NAT and Firewalls is that both can block incoming calls. To prevent them from doing so you can apply:

- Application Level Gateway
- Firewall Control Proxy

VoIP Call Setup Disruption

The two competing protocols for VoIP call setup are H.323and SIP. H.323 is a suite of several more specific protocols. It uses dynamic ports and binary encoding. SIP is a simpler protocol running over one port using a three way handshake. It uses a single port and text encoding.

Firewalls can block the call setup ports and NAT can change the IP address/ports being used internally. As a result they both disrupt the call setup process.

To prevent any such disruption, incorporate an ALG or FCP into the architecture that can manipulate the setup packet data.

What Should You Do Now?

Actions you can take now to protect your VoIP system include:

- Deploying Network Tools
- Protecting Voice Data
- Defending Against Registration Hijacking

Deploying Network Tools

You should create virtual LANs to separate voice and data traffic into distinct address spaces (physically unique networks are not required).

This protective measure helps to both reduce risk of data sniffers infiltrating the VoIP system and tune your IDS separately for voice and data.

Use firewalls designed for VoIP traffic.

At the voice gateway, which interfaces with the PSTN, disallow H.323, SIP, or MGCP connections from the data network.

Protecting Voice Data

Guidelines for protecting voice data as it travels over a VoIP network:

- Avoid PC-based "softphones" if practical
- Keeps voice and data networks separate
- Use access control and encryption where possible
- Use IPSec or SSH for all remote management and auditing access
- Do encryption at the router or other gateway, not the individual endpoints

Defending Against Registration Hijacking

The primary defenses against registration hijacking are to use strong authentication and to use VoIP-optimized firewalls to detect and block attacks.

At a minimum, all registrars should require MD5 digest authentication and selection of strong passwords. Passwords must not be "mechanically" generated (such as the extension with a prefix/suffix). These steps help to prevent dictionary-style attacks. Ideally, registrars should use strong authentication, such as that provided by the TLS.

The Internet Engineering Task Force (IETF)-approved security solution is to use the combination of TLS, MD5 digest, and strong passwords.

Registrations from the external network should be disabled if possible—or at least limited to a small set of external UAs (such as teleworkers), who have a valid need to register from the external network. Max-Forwards header limits (and other techniques) can be used to detect external attacks, but these limits not commonly enforced.

Of the numerous security issues unique to VoIP, registration hijacking is one of the more serious. An attacker who successfully hijacks registrations in your organization can block, record, and otherwise manipulate calls to and from your organization. This is a very real threat that you must counter.

Harden Your VoIP Against Attack

Consistent repair of your Common Vulnerabilities and Exposures (CVEs) is the litmus test that all information security professionals will be judged by regarding how successfully they are protecting their VoIP networks. Repairing vulnerabilities also helps you stay in compliance with related regulations, including GLBA, HIPAA, 21 CFR FDA 11, E-Sign and SOX-404.

CVE Management is the key to hardening your VoIP and removing defects from your computers and networking equipment. Three types of solutions that claim to help you harden your VoIP are:

- Configuration Management
- Patch Management
- Vulnerability Management

CVEs specific to VoIP are on the rise. By using an automated vulnerability management system to find and remediate them in a timely way, you can reduce the risk of your VoIP system being vulnerable to attack. If you find a solution that helps automate this process for you, make sure it helps find and fix CVEs. If the solution you choose has not been vetted by MITRE, then it may not be compatible with the CVE standard. MITRE is funded by the U.S. Department of Homeland Security to manage this industry standard—the database of exposures and weaknesses in all networking equipment and computers. Look for this logo to accompany the product or service in question verify it at http://cve.mitre.org.

Every day there are new CVEs listed and you can find them on http://cve.mitre.org, the homepage for helping you stop hackers and harden your assets. By knowing the CVEs, you can find any CVEs your VoIP system may have, then you can find a way to block any exploitation of that CVE that would impact your VoIP.

Protect Against CVE Exploiters

There are four key things you can do to protect yourself against CVE Exploiters:

1. Detect and track assets
2. Audit your VoIP for CVEs
3. Lock the doors against CVE Exploits
4. Clean up your CVEs

Detect and Track Assets

Do you have policies and systems in place to track all of your network-based assets? You should have a policy on whether or not you allow laptops in and out of the office. For instance, you may require that all laptops allowed on the network be company assets, rather than a personal computer that can be used at home. Do all hosts have the required firewall, antivirus, antispyware, and patches installed so they are up to date and have minimal vulnerability to attack? What about wireless routers and *ad hoc* wireless LANs—have you sniffed the airwaves and port connections to see if there are any new wireless devices or servers connected to your network? Answering these questions is critical in the protection of these assets against CVE exploiters.

Audit Your VoIP for CVEs

Find a tool you like. Google "Security Auditor" or use similar keywords and you'll find companies and products in this marketplace. Do an evaluation of open source versus commercial products. If you built your firewall from scratch, go for open source, otherwise find a company you can work with and trust. Make sure you pick a tool that doesn't take any assets off line, and one that scans and reports on CVEs.

Lock the Doors Against CVE Exploits

Your firewall is your best countermeasure. Make sure to review the firewall's logs—look for suspicious traffic. Also make sure you set up the VPN interface properly and know who's using it, whether they are coming in through a secure tunnel on an insecure or ***"sick"*** computer. By reconfiguring your rules table around CVE exploits, you can be one step ahead of the hackers. For example, why not block all inbound/outbound traffic for ports that you don't use—port 445 was exploited by MSBlast and Sasser. Do you need to keep this port open at the firewall? Look at the computers that have CVEs – how long will it take to fix those CVEs and what ports are they on? Update your rules table until it is fixed. Don't trust all patches. Reinspect your VoIP system the for same or new CVEs on the affected ports and services. Keep repeating this process, daily.

Clean Up Your VoIP's CVEs

Does your vendor offer patches? Did the patch fix the CVE? Yes, good. No? Then, why not shut off the service or feature that harbors the CVE – one quick configuration change like that and there won't be a CVE to exploit. Some CVEs can be patched while others require intelligent reconfiguration. Clean up your CVEs on the most important systems and highest risk of attack. Keep repeating this process, daily.

If you don't have time to do all this yourself, find a security appliance, service, or consultant who will do it for you. It's easy to find them, now that you know what to look for and where to look. It's a good idea to be sure that the security appliance or vulnerability management system, not only detects CVEs, but quarantines systems with CVEs until the issues are repaired in order to protect your VoIP network from intrusions. The system should then help with remediation and repair by providing some kind of tracking system.

CERT Recommendations

Carnegie Mellon University operates the CERT Coordination Center, a major reporting center for Internet security problems. CERT, founded by the Defense Advanced Research Projects Agency (DARPA), provides technical advice and:

- Coordinates responses to security compromises
- Identifies trends in intruder activity
- Works with other security experts to identify solutions to security problems
- Disseminate information to the broad community

The CERT/CC also analyzes product vulnerabilities, publishes technical documents, and presents training courses. In the CERT Advisory referenced above, recommendations are issued to help companies protect their networks from these vulnerabilities. Among their recommendations are the following:

- Block access to H.323 services on devices that do not need to be exposed
- Limit access to only those machines that use H.323 for critical business functions

- Limit access of any type to only those areas of the network where it is needed
- Consider disabling application-layer inspection of H.323 packets by Firewalls
- Coordinate among telephony, application, network, and desktop staff to assess the threat in individual network segments

Summary

VoIP security requires adapting traditional network security measures for a high speed, dynamic environment.

For information about how NetClarity ***Auditor*** can help you manage your VoIPs vulnerabilities, contact NetClarity at 781-276-4555.

For more information about VoIP, refer to the following resources:

- "Security Considerations for Voice Over IP Systems," NIST http://csrc.nist.gov
- "Five tips for securing a converged net," Computerworld http://www.computerworld.com/securitytopics/security/story/0,10801,85844,00.html?SKC=security-85844
- "Security in SIP Based Networks,"Cisco: http://www.cisco.com/warp/public/cc/techno/tyvdve/sip/prodlit/sipsc_wp.pdfIP
- Telephony Security in Depth–Cisco http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.htm
- http://cve.mitre.org
- http://www.sans.org/top20
- http://www.netclarity.net/
- http://netclarity.blogspot.com/

CREDITS:

Thanks to numerous NetClarity, Inc. customers for their time and suggestions for this document. Thanks also to NIST and CERT for providing information on their web sites.

Many thanks to the MITRE CVE team for their work in creating and standardizing CVEs, http://cve.mitre.org.