Enterprise Telecom Security Threats

A Corporate Whitepaper by
Mark D. Collier,
Chief Technical Officer and
Vice President of Engineering

Executive Summary

Corporations are typically connected to two public, untrusted networks: the Public Switched Telephone Network (PSTN); and Wide Area Networks (WANs) or the Internet. Traditional phone stations or peripherals connect to the PSTN to enable voice calls, modem and fax communications, and video teleconferencing. Corporate computers connect to WANs or the Internet for data communications and access to information. Internet Protocol (IP) phones and soft phones either connect to the PSTN via a media gateway, or cross the corporate perimeter to connect to WANs or the Internet. Although nearly all corporations secure the Internet connection to their internal data networks with IP firewalls and related technologies, most corporations have yet to lock down their voice connection to the untrusted PSTN, or when present, bring an equal level of security to their IP telephony connections.

An array of vulnerabilities in internal data networks, the traditional phone environment, and other critical corporate infrastructure are accessible through an enterprise's unsecured traditional phone network. Although attacks against an enterprise's Internet connection receive the most public attention, attacks against an enterprise through the traditional voice network are common. In a data network attack perpetrated through the traditional phone network, intruders bypass Internet-related defenses by using the PSTN to access unauthorized and poorly secured modems. Attackers exploit modems as interconnection devices between enterprise voice and data networks that enable cross-network attacks.

Unauthorized modem use is prevalent in many corporations, due to the logging and filtering of Local Area Network (LAN)-based Internet sessions by IP firewalls. The only means by which an employee can initiate a private Internet session, is through an un-monitored enterprise phone line connection to their personal Internet Service Provider (ISP). Once connected over the PSTN, users can access any content, engage in any transaction, or upload and download any information—completely invisible to the enterprise security or networking team. The vast majority of unauthorized modems are non-secure and poorly configured, because access to private Internet usage is the employee's goal—not security of the corporate LAN. Beyond these unauthorized modems, nearly all enterprise's have a collection of authorized modems for uses such as vendor maintenance port access into key networking infrastructure and building systems. A typical enterprise, even one with restricted modem usage policies and procedures, has some number of unauthorized and/or poorly secured modems—open "back doors" into their data network.

The traditional voice network is slowly migrating to Voice over Internet Protocol (i.e., VoIP, or IP telephony), where voice is a critical service running on the IP network. At this time, approximately 1% to 2% of telephone stations are based on VoIP. This migration will take many years, with most enterprises slowly rolling out the new technology by using a hybrid network consisting of both traditional circuit-switched and VoIP equipment. During this transition, the existing circuit-switched voice security threats such as attacks on authorized and unauthorized modems, toll fraud, and eavesdropping in the PSTN will continue—and VoIP will introduce entirely new vulnerabilities of its own.

Security is required for reliable VoIP deployment. Unfortunately, securing VoIP is more difficult than securing traditional, circuit-switched voice networks. With voice as a service on the IP network, it inherits both the advantages—and the disadvantages of the IP network. Now voice is vulnerable to worms, viruses, and Denial of Service (DoS)—all threats that did not exist on the circuit-switched network. For example, an attacker can use registration hijacking, proxy impersonation, message tampering, or session tear down to cause DoS on any VoIP network component, as well as Time Division Multiplex (TDM) systems. An attacker can also exploit common and well-known weaknesses in authentication; implementation flaws in software, protocols, and voice applications; weaknesses in IP PBX's general-purpose and non-secure operating systems and supporting services; as well as limitations in perimeter security devices.

VoIP is also harder to secure than other, traditional IP services. VoIP is very susceptible to DoS attacks, is comprised of complex, rapidly implemented "standards," and due to Network Address Translation (NAT), dynamic porting, and performance requirements, VoIP poses a problem for conventional perimeter security devices.

The vulnerabilities inherent in VoIP services expose the enterprise to some old threats present on the traditional voice network such as toll fraud and eavesdropping, but they also introduce new threats, such as attacks on IP PBXs, DoS on signaling and media, DoS on gateways and TDM systems, protocol attacks, call blocking, data tunneling and Quality of Service (QoS) theft, and attacks against IP phones, none of which were present with traditional voice implementations.

This document provides background on vulnerabilities in both traditional circuit-switched and VoIP implementations, as well as how different VoIP deployment scenarios are impacted by the threats. Vulnerabilities in a hybrid network consisting of both legacy circuit-switched and VoIP equipment are also discussed.

Table of Contents

1. Introduction

The vast majority of enterprises maintain a presence on the Internet in order to conduct business and provide Internet access for work-related activities. To secure the connection to the Internet and protect internal networks, enterprises deploy a variety of security devices, including firewalls, Virtual Private Networks (VPNs), Intrusion Detection/Prevention (IDP), anti-virus, and content monitoring. When properly deployed and configured, these products help to protect the internal IP network from attacks against the enterprise's Internet connection. However, none of these Internet-related security technologies protect the internal IP network from attacks

against the traditional voice network connections created by unauthorized or non-secure modems and poorly configured voice systems.

Furthermore, conventional measures taken to secure the data network are inadequate for voice traffic on the IP network, which cannot be subject o delays like those caused by standard firewalls. It is important for companies to take the necessary steps to provide a secure environment that addresses the unique vulnerabilities of IP telephony. [1]

2. Traditional Voice Vulnerabilities and Threats

Securing the enterprise's Internet connection is the focus of a great deal of security attention—and a warranted investment, because a large number of attacks come from the Internet. However, with so much robust technology protecting the Internet connection, many attackers search for pathways of penetration that are less likely to be detected. Unauthorized and non-secure modems offer an attacker that easy, unmonitored method of obtaining access to the internal data network, so they pose a serious threat to security.

Unauthorized and Non-secure Modems

When an attacker accesses an unauthorized or non-secure modem, the IP network-based security products cannot see or detect the intrusion. Typically, no record of the attacker's access is logged—except perhaps a long call recorded on the PBX—and even this record exists only if the accessed modem line routes through the PBX. Logs on the attacked system may record the access—but they are easily deleted by the attacker. The attacker can continue to re-use this newfound vulnerability for future access, or install another "back door," which allows access through another means, including the Internet.

As stated in September 2000 in the SANS Institute Resources, "Insecure modems, authorized or not, are vulnerable to such attacks and penetration of these modems will subvert the protection of firewalls." [3]

The following sections describe several situations exploiting unauthorized and non-secure modems within an enterprise.

War Dialing

Normally, an attacker uses "war dialing," the process of scanning a large set of phone numbers within an enterprise to pinpoint unauthorized and non-secure modems. The attacker easily obtains the enterprise's phone numbers using a phone book, social engineering, business cards, or even the Internet. Once the enterprise's range of numbers are obtained, the war dialer dials the numbers and searches for answering modems, recording the phone numbers of the answering modems for later attack. Some war dialers can identify the system controlling the modem and attempt to guess passwords. Any interested individual can download free war dialers from the Internet. Some of the more common freeware war dialers include Tone Loc, THC, Grim Scanner, Super Dial, Wild Dialer, and Ultimate War dialer 32. An attacker can even get a war dialer that runs on a Personal Digital Assistant (PDA) with a wireless modem.

When a war dialer finds a modem and guesses the username/password, the attacker has gained an unmonitored access point into the enterprise. From this point, the attacker can damage or manipulate the initial system, or since the system usually resides on a network, the attacker can access any other system in the network.

To further illustrate the problem, in the 1999 Computer Crime and Security Survey conducted by the Computer Security Institute (CSI) and the Federal Bureau of Investigation (FBI), of the almost 600 respondents, 28% reported modem-related security breaches. [4]

Peter Shipley amply demonstrated the problem posed by non-secure modems with a war dialing experiment that he conducted and later discussed at DEFCON (an annual "hacker" convention). In the experiment, he instructed his computer to dial 5.3 million phones in the San Francisco Bay area looking for computers connected to modems. He found numerous modems, including those that allowed him access to environmental controls and other critical systems. He further stated that 75% of the computer systems accessible via modem were non-secure enough for an intruder to penetrate the system.

Figure 1 provides a graphic from Signal magazine which illustrates the difference between what security managers perceive to be the greatest threat to their network and the reality that is often revealed by a vulnerability assessment is performed. The actual threat associated with modems is, in reality, much higher than generally realized. [2]

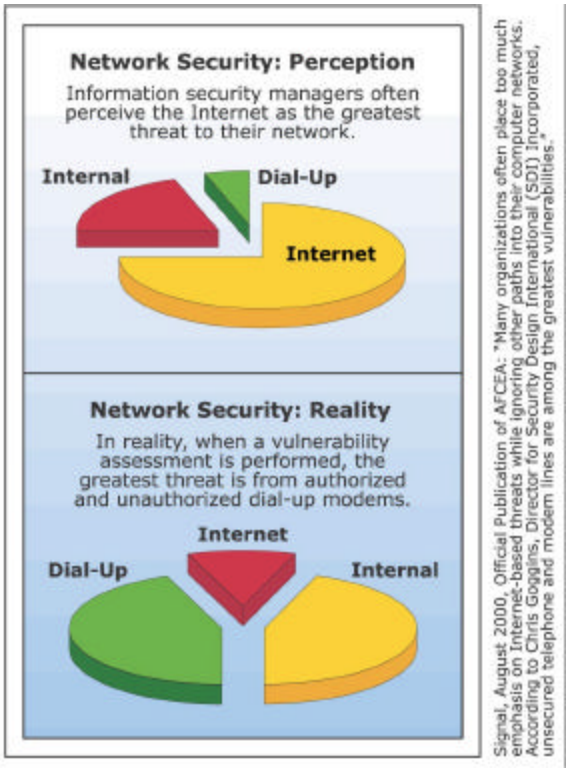

Figure 1 – Threat Level from Unauthorized Modem

Unauthorized Remote Access

In order to provide their remote users with access to the internal network, most enterprises invest in Internet-based VPNs and managed Remote Access Servers (RAS). Unfortunately, users often set up their own personal remote access. The reasons for this breach of security vary, but include a simple lack of awareness of the RAS, a real or perceived instability of the RAS, and a desire to work outside the monitoring of the VPN or RAS. Modern Personal Computers (PCs) make it easy for users to install a modem and personal remote access software, such as PCAnywhere. Users also provide backup remote access to a critical server by installing an external modem on the server's serial port. Although not always done with malicious intent, installation of unauthorized and non-secure modems create major security vulnerabilities for the enterprise. As stated in Information Security magazine, "one of the security professional's worst nightmares is the employee who activates an unauthorized modem on his desktop PC, installs a remote control program such as PCAnywhere (without a password), and turns on the modem before going home at night." [5]

Figure 2 illustrates this "back door" remote access into the enterprise LAN. Although the firewall monitors access from the Internet, the firewall cannot monitor access to the personal remote access modem.

When an attacker war dials the enterprise, finds the unauthorized remote access modem, and obtains a password, they have full access to the system. From this point, they can access data on the system itself, access other systems on the network, or install a trojan or other back door application.

Unauthorized ISP Access

Employee use of unauthorized modems for Internet access is a more common and serious problem. Many users are highly dependent upon the Internet for non-work-related activities, including access to entertainment, gaming, stock trading, Internet auctions, shopping, news, chatting, email exchange, and access/exchange of objectionable material. Most enterprises monitor employee access to the Internet, and many enterprises block Internet access by site or content.

This "need" for private Internet access, coupled with robust, IP-based Internet usage monitoring technologies, has greatly increased the number of unauthorized modems used for Internet access. Most users already have personal ISP accounts that they use when accessing the Internet from home. To reach the Internet from work, these users simply install a modem on their work computer and dial a local or 1-800 ISP. Although this unauthorized connection may be slower than the enterprise's high-speed Internet connection, the advantage of a completely unmonitored connection outweighs the inconvenience.

As stated in the SANS Institute Resources, "Unauthorized or uncontrolled desktop modems are a bigger threat to a business's security today mainly due to the changes in computer networks." [6]

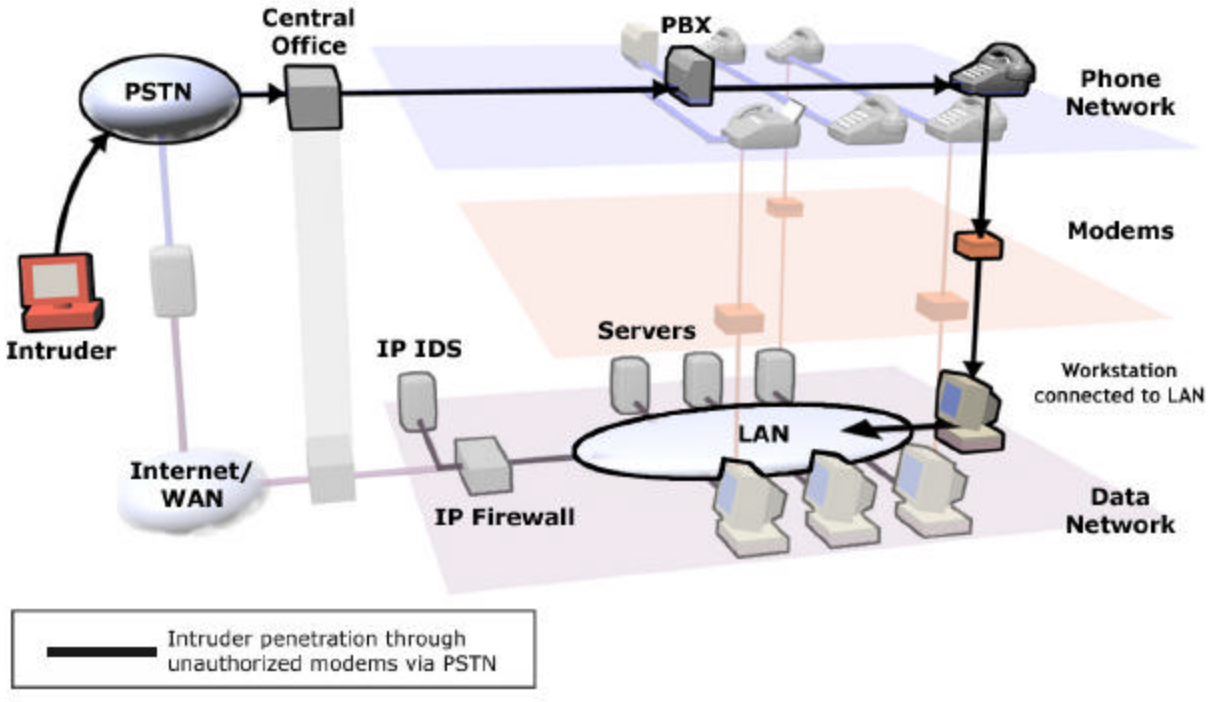

Figure 2 – Unauthorized Remote Access Modems

When a user accesses the Internet through an ISP, they intentionally or inadvertently create a completely unmonitored connection that can:

- Provide an attacker with unprotected access for a cross-network attack on the internal data network. The connection is found, and vulnerabilities are exploited using IP port scanning.
- Transfer proprietary or classified data to their ISP.
- Access a non-enterprise email account and download worms/viruses and other software with malicious content.
- Access objectionable material and place it on the enterprise network.
- Tie up expensive voice channel bandwidth during the session.
- Spend unproductive time using the Internet for non-work related activities.

Employee abuse of Internet access privileges is quantified in the 2004 CSI/FBI Computer Crime and Security Survey. Of the almost 500 respondents (primarily financial institutions, large corporations and government agencies), 59% detected employee abuse of Internet access privileges, for an estimated loss of $10,601,055. [8]

One government security administrator found that unauthorized ISP access consumed 28.5% of the local access voice circuits during peak hours. In this case, unauthorized ISP access consumed almost three full T1 circuits (72 total voice channels). Security concerns aside, this is a tremendous waste of expensive voice bandwidth. Typically, voice T1 circuits cost $1,000 per month. Elimination of this sort of unauthorized activity saved the site approximately $36,000 per year.

Another negative effect of unauthorized ISP access occurs when an enterprise tries to rid itself of a virus or worm. Users reintroduce the virus via their personal accounts over their modem connections, so the virus/worm continues to reappear despite upgrades to their network-based mail scanning software and laborious PC and server purgings.

Truly serious conditions occur in highly secure areas where Internet access is prohibited, but the restriction cannot be effectively enforced. Under these circumstances, users gain unauthorized access to the Internet by connecting modems to telephone lines. In doing so, the user places a highly secure system and its network on the Internet. The user can upload sensitive or classified material to their ISP or inadvertently provide an Internet-based attacker with access to their system.

Figure 3 illustrates the use of unauthorized modems for ISP access. By accessing the Internet with an unauthorized modem, the user circumvents the IP firewall and places their system and the enterprise's network directly onto the Internet.

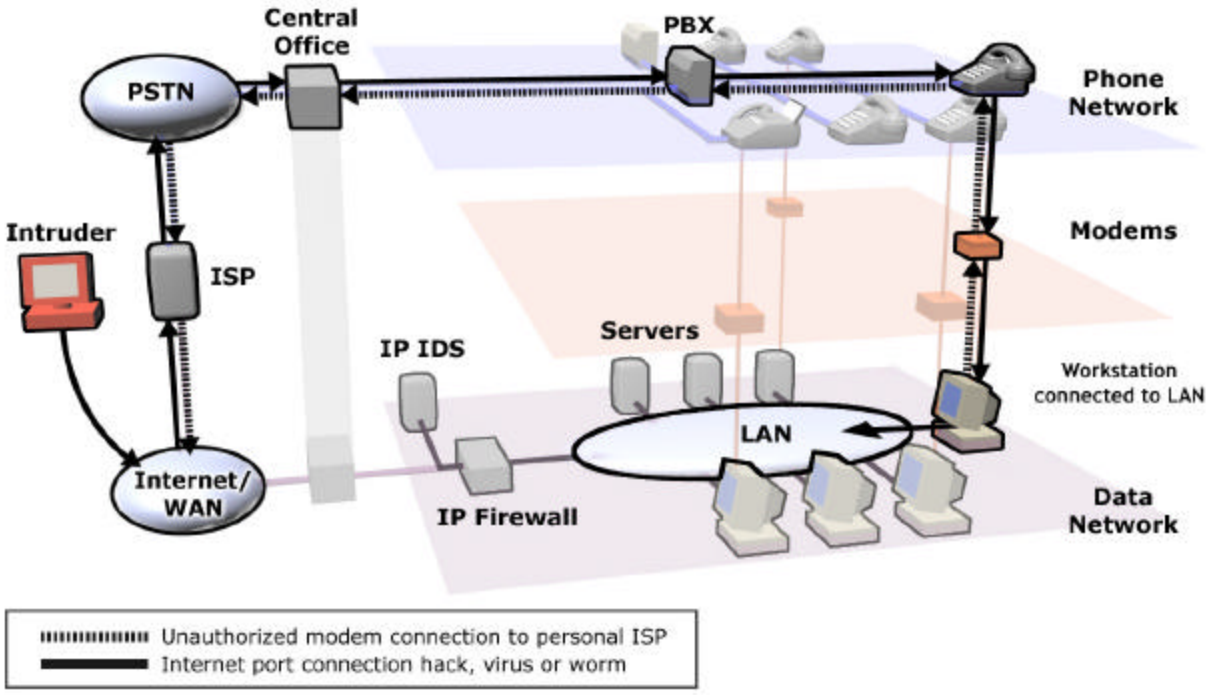

Figure 3 – Unauthorized ISP Access

Unsecured Authorized Modems

All enterprises have some number of authorized modems. Critical systems such as large computing, voice, and infrastructure systems often use modems to provide remote access for technicians or data acquisition/control for a Supervisory Control and Data Access (SCADA) system.

Although many enterprises protect their critical system modems, most do not. Large enterprises often have hundreds of authorized modems, and it is difficult to efficiently enforce a corporate policy across a large number of modems. Although strong passwords, dialback capability, and other techniques are used to try to protect authorized modems, these are individually managed point solutions that are difficult and expensive to manage on a large scale, and inevitably lead to some number of poorly protected modems.

Non-secure, authorized modems are an issue not only because of their large numbers, but also because of the criticality of the systems using the modems. The modems are present to provide maintenance or access/control for what is typically a complex and critical system. Therefore, any unauthorized access can have serious results. An attacker can disable a PBX or use it for toll fraud, steal data from servers, manipulate environmental systems, affect critical infrastructure, etc. The potential for damage and misuse is an issue even if the attacker cannot use the system as a jumping point to another system or a cross-network attack.

Figure 4 illustrates an attacker accessing non-secure authorized modems. As shown in the figure, non-secure authorized modems can provide access to data networks, voice networks, and other building systems.

SCADA systems are especially vulnerable. For example, utilities use modems for access and control of their remote stations. Access to these systems can result in disruption of electrical power, gas resources, water supply, and other critical services. This is a very serious issue, and attackers are likely to exploit it heavily in the future as heightened security prevents other means of attack.

The U.S. Department of Energy conducted a demonstration at several SCADA sites in April 2004. Detailed data is sensitive, but the security analysis summary states that unprotected remote access modems offer almost no defense again attacks and are easily identifiable by novice attackers using tools freely available on the Internet. It goes on to say that attacks against remote access modems could easily lead to exposure or compromise of sensitive information, and eventually, complete access to the automation system resources.

Attacks Against Traditional Voice Systems and Services

Toll Fraud

Although modems are not directly involved, the voice network provides an avenue of attack against critical voice systems. Attackers can place a standard call and use Dual Tone Multi-Frequency (DTMF) tones to access and manipulate PBXs, Interactive Voice Response (IVRs), Automatic Call Distribution (ACDs), and other systems in order to commit theft of long-distance services, or create other issues. By war dialing, attackers find lines and codes that provide a second dial tone, which they use to commit toll fraud.

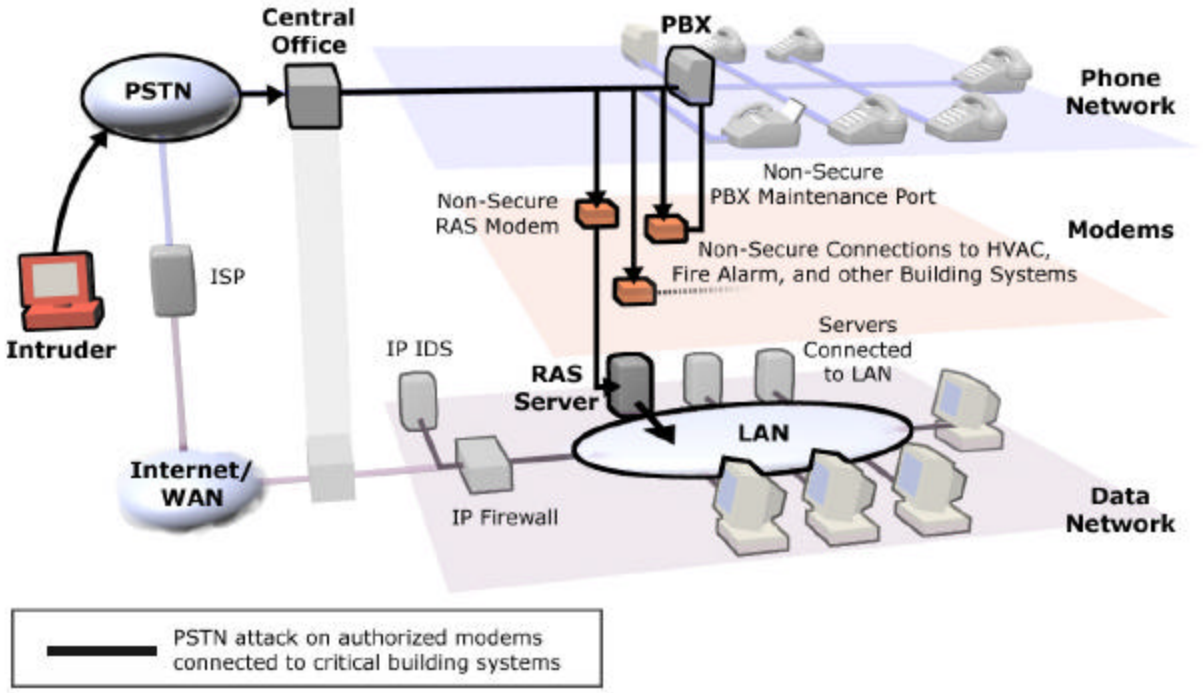

Figure 4 – Non-Secure Authorized Modems

Some enterprises enable Direct Inward Service Access (DISA), which allows a caller to gain an outbound dial tone. Passwords can be enabled with DISA, but they are often weak and once determined, can be "sold" to facilitate toll fraud. It is also possible to war dial an enterprise and scan for DISA tones, which can then be easily exploited.

This is not a new problem, and it continues to impact business operations for enterprises. Other attacks include use of DTMF to guess passwords and access voice mail and other voice systems. Consider the example with Hewlett Packard, where an extremely sensitive voice mail was extracted from an executive's voice mailbox.

In 2003, the Communications Fraud Control Association (CFCA) estimated annual telecom fraud losses worldwide to be in the range of $35-$40 billion U.S. dollars—up from the previously estimated $12 billion. The estimate was based on the results of a comprehensive opinion survey of telecom companies in 26 countries. Of the 20 to 30 different fraud types identified by the respondents, PBX/PABX/Voice Mail/CPE fraud (i.e., theft of long distance services by an unrelated third party by penetration or manipulation of Customer Premise Equipment) was ranked #2 and increasing. [9]

Figure 5 illustrates an attacker accessing and exploiting the various voice systems and services that are vulnerable to attack.

Eavesdropping

The vast majority of voice traffic is not encrypted in any way, so it is possible to intercept and eavesdrop on conversations in the PSTN. Furthermore, this vulnerability is increasing in severity with the rapid transition of the PSTN from a circuit-switched network to a packet-based network.

Clearly, the U.S. Government recognizes this vulnerability, because it has countered the threat by building dedicated voice networks and using approximately 500,000 secure phones to encrypt voice calls. These secure phones are point-to-point encryption devices called Secure Telephone Units (STUs) and Secure Telephone Equipment (STEs). The STUs and STEs are effective when manually activated by the user, but fall short as an effective overall solution, since each person conducting a classified or sensitive conversation must have access to a device.

The same eavesdropping vulnerability that the U.S. Government recognizes also exists for commercial enterprises. Commercial secure phones are used to encrypt conversations for enterprises, and executives use these phones for international calls, secure faxes, and secure video conferencing.

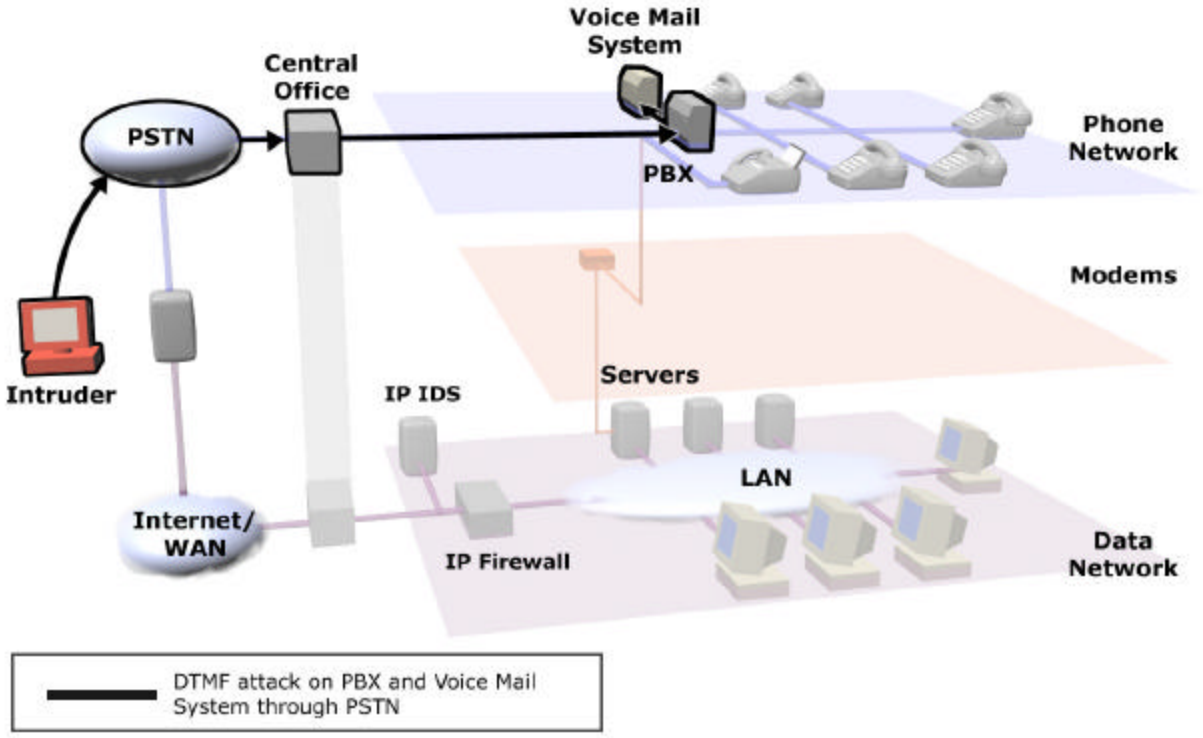

Figure 5 – Voice System Attacks

3. VoIP Vulnerabilities and Threats

VoIP is the future for voice communications, but successful VoIP deployment requires strong security. If the VoIP network is not secure, the expected levels of quality and reliability cannot be maintained. The challenges inherent in securing services on a shared IP network make securing a VoIP network much more complex and arduous than securing a traditional circuit-switched voice network. For instance, VoIP is vulnerable to traditional IP attacks—worms, viruses, and DoS—and is only as secure as the weakest link on the network. VoIP services are provided via IP PBXs running on non-secure operating systems with non-secure supporting services (such as databases and web servers). These operating systems and services are susceptible to the same attacks that regularly knock out other types of servers, making the IP PBXs more vulnerable than traditional PBXs.

Securing VoIP is also more complex and arduous because it involves more components and software than a traditional circuit-switched voice network. In fact, VoIP has the potential to double the number of IP devices on the network, thereby doubling the number of access points into the network. VoIP components include IP PBXs, supporting servers, media gateways, switches, routers, firewalls, cabling, and IP phones/softphones. More components mean a greater potential for vulnerability —and VoIP components often use general-purpose operating systems, which tend to have more vulnerabilities than purpose-built operating systems. If not properly secured, each endpoint, IP phone, and softphone is susceptible to attacks such as registration hijacking, toll fraud, eavesdropping, and malicious code—from both outside and inside an enterprise.

VoIP is also a greater challenge to secure than other, more traditional IP services. There are several characteristics and requirements unique to VoIP that make providing security much more difficult. For example, VoIP has unique real-time and reliability requirements that make it highly susceptible to DoS attacks, yet intolerant of any security feature that adds latency. Any delay of the media by as much as .5 of a second makes a conversation unusable.

Unfortunately, traditional data security devices are not designed to adequately address the real-time requirements of voice communications. Most firewalls slow data transfer, impeding the flow of traffic and adding an unacceptable latency to RTP packets. VoIP requires up to six additional ports to be opened for the duration of each call: two well-known signaling ports (one for each direction), as well as two ports for the media, and, optionally, two more ports for RTCP, which monitors performance. Conventional firewalls were not designed to handle this type of complex traffic. Nor are they designed to monitor VoIP signaling for attacks against the voice network. Without inspection at the application layer, firewalls have to open these several ports per call without determining whether the packets are legitimate, leaving the IP PBXs and IP phones vulnerable to external attacks such as DoS and toll fraud.

Figure 6 illustrates that traditional data firewalls control which services pass through the corporate perimeter, but by failing to monitor VoIP traffic at the application level, leave a security gap through which IP PBXs, IP phones, and other components are exposed to attack.

Based on interviews with companies that have installed IPT [IP Telephony], Forrester found that most companies fail to consider the unique vulnerabilities caused by integrating voice into a converged network prior to deployment. Although most companies take major steps to regularly upgrade their data networks to prevent attacks, many fail to recognize the need to add additional security measures when adding voice traffic to the data networks. Only 25% of the companies interviewed upgraded or replaced

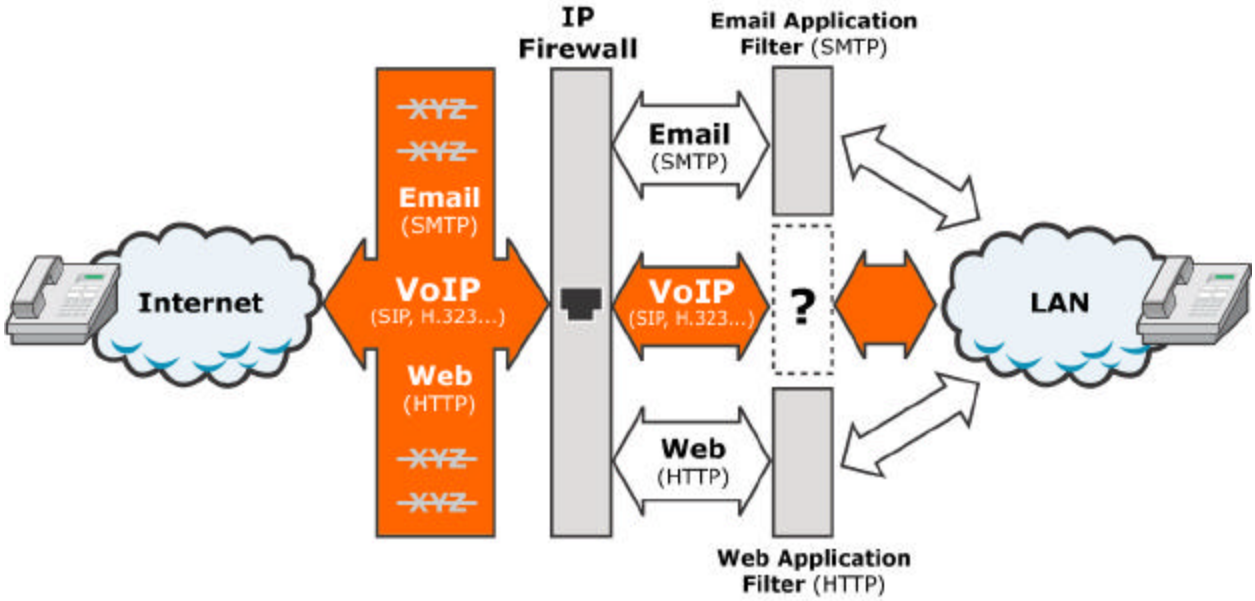

Figure 6 –Security Gap Left by Traditional Data Firewall

firewalls and just 22% changed to secure gateways. Companies that do not address security requirements…risk exposing their data networks to malicious attacks from external or internal sources. [1]

VoIP is also more difficult to secure than other, more traditional IP services because VoIP consists of many complex "standards" that are both dynamic and, due to a "rush to market," often poorly implemented. There are many VoIP "standards," including the Session Initiation Protocol (SIP), H.323, MGCP, H.248, and vendor-proprietary protocols/versions. H.323 and SIP are two leading protocols used for VoIP. H.323 is the most commonly used today, but SIP is considered the future protocol for VoIP; the universal protocol to integrate the voice network and provide the foundation for new applications.

However, it is very difficult to secure a SIP system with the current state of SIP implementations. As an emerging and relatively immature standard, SIP does not have clearly defined security requirements. The lack of firm specifications on SIP standards allows vendors to determine how much security to build into the system. Unfortunately, SIP does not offer any built-in security. Most SIP development has focused on feature sets and interoperability, with limited attention paid to security. Even if one vendor's components do support security, all other participating components must also support security in order for it to be used.

VoIP standards are complex, and many implementations have flaws (i.e., programming mistakes), which lead to vulnerabilities. For instance, an implementation flaw such as not properly checking the size of a protocol request can be exploited by an attacker to achieve unauthorized remote access or a DoS attack.

Vulnerabilities are also a result of vendor "rush to market." Protocols can be either implemented by the vendor (i.e., it is up to the vendor to focus on building a secure implementation), or purchased from a "stack" vendor (in which case vulnerabilities are shared among any system using the stack).

An example of vulnerabilities resulting from an implementation flaw that was shared among multiple vendors—and even a vendor's multiple products—is a security flaw in a widely replicated implementation of the H.323 protocol that was discovered by researchers at the University of Oulu in Finland. In January 2004, Microsoft conceded that users of the NetMeeting software were probably vulnerable to the buffer overflow bugs found in implementations of the H.323 VoIP protocol, which could allow a remote attacker to take control of affected systems. (The flaw was previously addressed in Microsoft's Internet Security and Acceleration server software.) Microsoft was only one of a large number of vendors impacted by the H.323 implementation flaw. [10]

Figure 7 illustrates the basic layers of software used in an IP PBX—any of which can have vulnerabilities.

The above challenges entailed in securing the VoIP network leave VoIP vulnerable to several threats, including eavesdropping, DoS on signaling and media streams, DoS on gateway and existing TDM systems, attacks exploiting weaknesses in the various protocols, data tunneling, attacks exploiting weaknesses in IP PBX implementation, unauthorized access to IP PBXs, and attacks against IP phones/softphones. Additionally, VoIP is vulnerable to more severe attacks against various voice services, such as toll fraud, voice mail attacks, and call manipulation. The remainder of this section focuses on the vulnerabilities found in the majority of vendor implementations, attacks that exploit the vulnerabilities, and the level of threat impacting common VoIP deployment scenarios.

SIP Vulnerabilities

Some SIP/VoIP vulnerabilities result from the underlying computer system platform, implementation bugs, and the IP network (media attacks). SIP systems can be attacked directly or indirectly by viruses/worms, which affect the underlying operating system, the database, web server, or other supporting software. A SIP system can be attacked through an implementation flaw in any software component, including the SIP "stack" or application. This section focuses on inherent SIP vulnerabilities present for the majority of vendor implementations, such as registration hijacking, proxy impersonation, SIP message tampering, session tear down, DoS, and NAT issues.

Registration Hijacking

A rogue device can register itself and receive incoming calls intended for a legitimate phone. Registration hijacking describes when an attacker impersonates a valid User

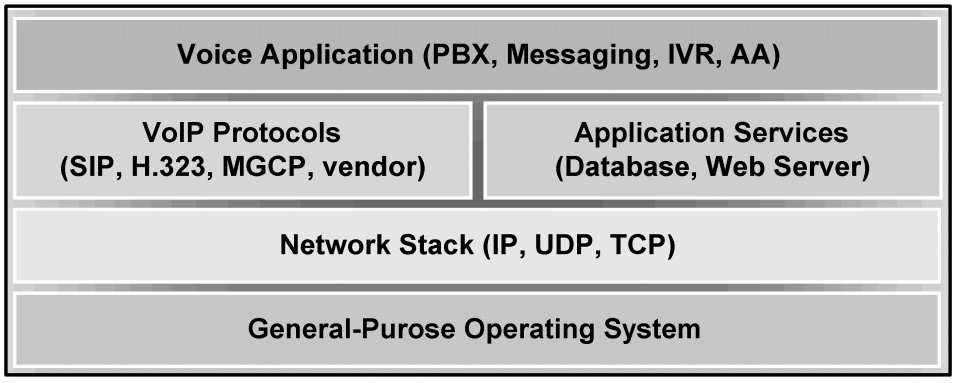

Figure 7 – Typical IP PBX Software Stack

Agent (UA) to a registration server, and then registers itself, causing all requests intended for the legitimate UA to be directed to the attacker instead.

Registration hijacking can result in toll fraud, where toll calls are relayed to a media gateway. An automated attack could generate many calls, resulting in huge charges or a DoS condition against a gateway or PBX. Attackers can also redirect all incoming (phone) or outgoing (gateway) calls via their UA to eavesdrop or monitor calls.

Registration is commonly performed using User Datagram Protocol (UDP), which is non-secure. Authentication is often not required, in fact, registration servers are only "RECOMMENDED" to challenge UAs for authentication. Even when authentication is used, it is normally weak (a username and password, sent in the clear). Strong authentication can only be used if all participating components support it.

Compromised SIP phones can be used to recover passwords for use in registration hijacking or guessing passwords. Compromised soft phones may also be used to find passwords. If passwords are either set to a default or generated mechanically (e.g., "company-1234" for extension 1234), an attacker may be able to guess other UA passwords. Dictionary-style attacks are also able to recover strong passwords. Additionally, an internal or external attacker can "fish" for registerable UA addresses to build a directory.

Proxy Impersonation

A phone or proxy server can be tricked into communicating with a rogue proxy server. Outgoing calls from a UA are sent either directly or via intervening proxy/proxies to a proxy in the domain of the called party. Proxy impersonation describes the situation where an attacker's proxy intercepts these calls. Proxy impersonation can occur through packet interception, domain registration hijacking, and Domain Name Server (DNS) impersonation, allowing an attacker to eavesdrop, track, redirect, and block calls.

By impersonating a proxy once, an attacker can forge "301 Moved Permanently" responses, which causes the caller and intervening proxies to use an attacker's proxy instead of the originally intended proxy. By impersonating an organization's proxy, attackers can redirect incoming SIP calls via their UAs to eavesdrop and track calls, or perform selective and wholesale DoS.

Message Tampering

Message tampering occurs when an attacker intercepts and modifies packets between proxies. UAs may secure SIP messages using Secure Multipurpose Internet Mail Extension (S/MIME) to authenticate and optionally encrypt their text, with only those portions needed to deliver the packet remaining in the clear. Even with S/MIME, attackers may tamper with routing information to confuse proxies (e.g., they may include broadcast addresses or loops in an attempt to overload servers).

Message tampering can cause users to be billed incorrectly for calls, and can mask toll fraud attacks. By modifying packets, attackers can redirect all incoming calls via their UAs to eavesdrop on the calls. Attackers can also block calls, or send unexpected calls through media gateways, which can tie up TDM trunking or switches. Additionally, attackers can use message tampering to redirect future SIP calls via impersonating proxies, which can continue to track calls after the attack is completed or defeated.

Session Tear Down

Once a call is established, either party can modify or end it. If attackers observe the initial messages, they can forge a BYE or re-INVITE message to shut down or alter the session. The latter case allows the attacker to redirect media, which allows eavesdropping. In general, teardown messages from an attacker are impossible to prevent, because the necessary fields must be sent in the clear to allow routing.

Loss of service is the primary affect of session teardown and is a likely result of incorrectly implemented attempts to reestablish sessions to implement eavesdropping. Redirecting media to broadcast addresses could cause a DoS attack. Redirecting media sessions to a media gateway could cause a DoS attack on the gateway.

DoS

Denial of service occurs when an attacker sends a well-crafted packet to the target system, causing it to fail, resulting in a loss of function for an IP PBX or other VoIP component. DoS also occurs when an attacker causes a flood of packets to be sent, overwhelming the target and preventing it from handling legitimate requests.

DoS against a SIP system is simpler to achieve than DoS against other data systems, due to the QoS requirements of VoIP. DoS against a SIP system can occur through registration hijacking, proxy impersonation, session tear down, message tampering, or these additional means:

- Weak authentication on proxies forces them to handle signaling packet floods.
- Using DNS to resolve remote hosts is proposed for SIP address resolution over the Internet. If the DNS server has incorrect data or has failed, a DoS condition results.
- DoS can result in targeted or large-scale loss of function for the SIP system. A compromised PC can forge "Vias" and create redirection to a non-existent host or a circuit "Via" path. Using broadcast addresses causes traffic amplification.
- SIP requires firewall ports to be opened for UDP streams, allowing possible flooding of UAs. Weak authentication mechanisms force UAs (including media gateways) to handle UDP flooding. Firewalls must make fast, intelligent decisions about which UDP ports are in use by valid SIP calls.
- Firewalls determining which UDP ports are in use by SIP traffic and which ports should be denied could be slowed if UDP streams are sent to random ports, consuming all processing resources by forcing the firewall to determine the state of all UDP ports.

The 2003 CSI/FBI Computer Crime and Security Survey reported that DoS had risen to be the second most expensive computer crime among survey respondents. [7] In the 2004 survey, DoS emerged as the most expensive computer crime (replacing theft of proprietary information, which had been the leading loss for 5 consecutive years). The combined DoS losses for both years exceeded $91 million. [8]

Considering the currently small percentage of VoIP deployments, DoS attacks against VoIP systems cannot yet be a significant contributor to these statistics. However, considering DoS against a SIP system is simpler to achieve than DoS against other data systems, the 2003 and 2004 surveys paint an ominous picture of future DOS attacks on non-secure voice services.

NAT Transversal Issues

NAT is an Internet standard that enables a LAN to use one set of IP addresses for internal traffic and a second set of addresses for external traffic, allowing the enterprise to shield internal addresses from the public Internet. NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network. NAT is common in the current IPv4 Internet, and is essential in dealing with the limited address space problem present with IPv4.

SIP ignores the existence of NAT and assumes end-to-end delivery of packets. The Session Description Protocol (SDP) layer of SIP communicates the IP addresses of media endpoints between UAs. If NAT modifies the IP addresses, connections cannot be made, so Back-to-Back User Agents (B2BUAs) straddle a NAT at the perimeter and modify SDP to enable the connection.

To be able to modify IP addresses, B2BUAs require SDP to be unencrypted and unauthenticated. When B2BUAs are used, it is impossible to use S/MIME to secure signaling, so a large range of attacks are possible, including registration hijacking, proxy impersonation, session tear down, message tampering, and DoS, plus attacking the B2BUA to gather the signaling data it processes.

IP PBX Vulnerabilities

IP-enabled PBXs are traditional systems using a TDM-based switching fabric. IP PBXs (also described as client/server, call managers, media servers, etc.) are server platforms running Windows, Linux, or some variant of Unix, which provide voice services solely on the IP network and require a media gateway for communication to the PSTN. Additional servers provide redundancy or other applications such as voice mail and presence.

The most critical vulnerabilities are those present on IP PBXs—which are the heart of any VoIP network. Due to both their critical role in providing voice service and the complexity of the software running on them, IP PBXs are the primary target for attackers. An IP PBX's multiple vulnerabilities are discussed below.

Non-Secure Operating System/Support Services

IP PBXs run commercial operating systems including Windows 2000, Linux, and variants of Unix, each of which carry well-known vulnerabilities typically accessed through network services. The number of vulnerabilities depends on the operating system, its version, and which network services are present/enabled. For example, the Cisco Call Manager runs on Windows 2000 and has a history of vulnerabilities.

Most IP PBXs run supporting services, such as a web server or database. These services are used over the network, and like the operating system, can be exploited. For instance, the Cisco Call Manager uses IIS and SQL Server, which have known vulnerabilities. The "Code Red" virus is an example of an attack that targets IIS, and the SQL Slammer worm is an example of an attack that targets SQL Server.

Operating system and support service vulnerabilities can be exploited to cause a failure, or allow unauthorized access, enabling configuration modification and access to sensitive data, including voice mail messages and CDR.

Unauthorized Administrative Access

IP PBXs are managed through a web-based interface or network client. If the authentication method is compromised, an attacker has administrative access to the IP PBX. If a web server or client uses a weak protocol to exchange authentication information, it is possible to collect and exploit it.

Voice Application Implementation Attack

Vulnerabilities also exist in the actual voice applications, which accept signaling requests from the network (in some cases an external network). Because the voice applications are feature-rich, there will be the similar types of implementation vulnerabilities. This will continue as standards evolve and grow in scope. Vendors will be constantly working to keep up with these standards and their implementations will include vulnerabilities. Large vendors are likely to have their own implementations and the smaller ones will use protocol stacks from other vendors as building blocks. When a vulnerability is found, it will impact many users and possibly multiple vendor implementations.

Voice application vulnerabilities can be exploited to cause a DoS, provide unauthorized access, or perform unauthorized actions such as terminating a call, allowing a toll call, or impacting a user's phone services. If unauthorized access is obtained, access to configuration and data is also possible.

Voice Application Manipulation

Voice applications will also be vulnerable to signaling manipulation or attacks against weak authentication. For example, unauthorized users will access toll lines, listen to voice mail, and manipulate presence. Most of the authentication information from IP phones is either weak and/or sent in the clear. If attackers can authenticate themselves as a privileged (or important) user, they will have access to that user's service.

Network and Media Vulnerabilities

VoIP transport is provided across the LAN, WAN, and Internet. VoIP administration, call control signaling, and the voice media travel over the same physical network as other IP services, consisting of switches, routers, firewalls, and cabling. IP phones exchange signaling with IP PBXs to establish calls, but call media is exchanged directly between IP Phones. Although its components are less vulnerable than IP PBXs, as described below, the network itself can be exploited to impact voice services.

DoS on Signaling

VoIP network components that accept signaling are vulnerable to DoS. If an attacker generates a flood of certain signaling requests (e.g., call setup requests) to a IP PBX, media gateway, or IP Phone, the targeted device will

be unable to efficiently process legitimate requests. The actual level of vulnerability depends on device set up (i.e., authentication scheme, whether Virtual LANs (VLANs) are used, etc.). If IP softphones are allowed, a rogue application could exploit this vulnerability.

Signaling DoS attacks on media gateways can consume all available TDM bandwidth, preventing other outbound and inbound calls and affecting other sites that use TDM. For example, certain entertainment providers who set up TDM 1-800 numbers for voting were impacted by individuals generating hundreds or thousands of VoIP requests through a broadband service provider, which in turn converted them to TDM and sent them on.

DoS on Media Sessions

DoS on media is a serious problem. VoIP media, which is normally carried with RTP, is vulnerable to any attack that congests the network or slows the ability of an end device (phone or gateway) to process the packets in real time. An attacker with access to the portion of the network where media is present simply needs to inject large numbers of either RTP packets or high QoS packets, which will contend with the legitimate RTP packets.

VoIP media sessions are very sensitive to latency and jitter. They are sent point-to-point and, other than media gateways, do not typically go through IP PBXs. VoIP requires QoS on the network, which requires a switched connection and a scheme for prioritizing voice traffic. VLANs help provide QoS and aid security.

An attacker with access to the network where the media sessions are active, and who can generate packets with high QoS labeling, will impact the media sessions. The most vulnerable parts of the network are shared segments, such as the WAN or untrusted long-haul network. The amount of high QoS traffic allowable on a shared WAN is finite and vulnerable to DoS.

Eavesdropping

Users expect voice calls to be private, as opposed to email or Instant Messaging (IM), where there is not usually an expectation of privacy. Although some VoIP calls are encrypted, most are not. Additionally, encryption without strong authentication cannot guarantee privacy, because participants can't be sure an attacker is not accessing the media by performing a Main-In-The-Middle (MITM) attack. If an attacker gains access to unencrypted media, simple tools such as VOMIT, which converts an IP phone conversation into a .WAV file, can be used to listen to or distribute audio.

If an attacker has access to the portion of the network where a call is being transported, the call can be recorded using a packet sniffer or MITM application. A packet sniffer records packets and saves them to a file. A tool such as VOMIT converts the packets into a .WAV file that can be distributed and played. A packet sniffer can collect media as well as signaling, which can include tones, such as DTMF tones used for account codes. The majority of VoIP installations use switched Ethernet networks, often with VLANs, making it more difficult to sniff packets.

VoIP calls taking place within the LAN are as vulnerable to eavesdropping as other communication services, such as email and IM. Traditional voice calls are "perceived" to be more secure and more suitable for sensitive communications because traditional (and VoIP) calls use real-time protocols, as opposed to store-and-forward protocols.

MITM attacks can also occur and defeat encryption on the IP phone. For example, the MITM application acts as the IP PBX, interacts with the real IP PBX, and "tricks" the source and destination IP phones into sending the media to an application that can record it. In this case, the call signaling and media can be recorded, monitored, and manipulated.

Data Tunneling

As VoIP connections are set up to an untrusted network, additional ports must be opened in the perimeter firewall. As commonly occurs with port 80 (HTTP), other services will "tunnel" through the new VoIP ports. These apparent "voice" calls will be data calls, tunneling through the firewall and wasting high QoS bandwidth. This same issue exists for the WAN, where precious high QoS bandwidth is wasted by data calls. Basically, these are new generation modems, which must be detected and terminated in order to maintain QoS.

IP Phone/Soft Phone Vulnerabilities

IP phones are specialized computers designed to provide voice service over the IP network and use embedded application-specific or general-purpose operating systems. Softphones are applications that run on PCs and provide a phone interface and functionality. Specific vulnerabilities are being found on IP Phones at a faster rate than on IP PBXs, mainly because the phones are fairly cheap and easy for hackers to set up and experiment with. Similar vulnerabilities exist with IP softphones because vendors often use very similar software.

IP Phones and softphones are the least critical part of the VoIP network, but they are also the most common and least controllable components. This is especially true for IP softphones, which are applications running on PCs.

While IP Phones are fairly new, there are many vulnerabilities present, virtually all of which are common on other IP devices. This is alarming, because it indicates security has received a low priority. Phones run general-purpose operating systems and must support rich signaling as a basis for new applications. They are also inexpensive (check eBay for IP phones) and easy for attackers to acquire and experiment with. Studies such as the one at www.sys-security.com, although slightly dated, accurately illustrates the types of issues present with some phones.

The specific vulnerabilities discussed in this section have been or can be fixed, but the user is required to patch the software on the IP Phone. Similar vulnerabilities exist with IP softphones because vendors often use very similar software. IP phone/Soft phone vulnerabilities include:

Unauthorized Remote Access

Multiple IP Phones, including those from Cisco (when using "Skinny") and Pingtel, provide a web server for administration. The web servers use base64 encoded username/password pairs, which if retrieved from the network, are easily decoded.

The Pingtel IP Phone ships with no administrator password for the "admin" account, and the account name cannot be changed. If a password is not implemented, an attacker can gain both remote and local administrative access.

Multiple IP Phones, including those from Cisco and Pingtel, provide a Telnet server. For both types of phones, abuse of the Telnet feature provides operating system level access. Telnet abuse leads to full access of the IP Phone operating system.

Administrative access to the IP Phone allows attacks beyond DoS. For example, when using SIP, a MITM proxy can be configured, giving the attacker access to the signaling and media streams, which is a more likely means of obtaining signaling and media than sniffing.

The Cisco ATA-186 analog telephone adapter interfaces analog phones to a VoIP network, and can be configured via a web interface. One version of this device displays its configuration screen—with password—if sent a single byte HTTP POST. Such commands can be used to reconfigure the device.

DoS

For multiple IP Phones, an authenticated user can change settings to create a DoS condition for the IP Phone. For example, Cisco IP Phones can be forced to restart by using common DoS applications, including "jolt," "hping2," "trash," etc. Cisco IP Phones can also be made to restart if sent a specifically constructed HyperText Transfer Protocol (HTTP) request. Any active call will be terminated in this case.

For specific Pingtel IP Phones, an authenticated user can reset the phone, which requires 45 seconds to reset. Certain values can be set which prevent the IP phone from rebooting, which requires a local update. If exploited for hundreds or thousands of phones within an enterprise, a great deal of effort would be required to recover.

Unauthorized Local Access

IP Phones are very vulnerable if an attacker has physical access to the phone itself. Most IP Phones authenticate themselves either only once or periodically, and do not require authentication for each use (which would be unacceptable for the average user and for 911 situations). IP Phones are highly programmable, so an authenticated user can transfer, block, forward calls, etc. Additionally, an attacker with local access can install a hub between the IP Phone and the switch and eavesdrop on packets.

The Cisco IP Phones locally store their configuration. Most of this data is accessible via the "Settings" button. By default, these settings are locked, but can be modified via a documented, but non-configurable special key combination "**#".

The Pingtel IP Phones can be reset to defaults, changing network settings without requiring authentication. During authentication, a potential attacker can view the password, which is displayed prior to being replaced by an asterisk.

Protocol Implementation Attack

As previously discussed, protocols such as SIP have inherent vulnerabilities. For example, an attacker who gains visibility into the signaling between two IP Phones can issue CANCEL or BYE requests, which effectively create DoS against one or both phones. The attacker can also provide certain return codes which create a DoS or allow a MITM attack. These vulnerabilities can only be used if the attacker has visibility into the signaling, so as to know when to generate the appropriate requests or responses.

Unauthorized Firmware Upgrades

Virtually all IP phones are programmable and can be upgraded with new firmware. For instance, Cisco phones are upgraded through Trivial File Transfer Protocol (TFTP), which is not secure and allows a trojan or rootkit to be placed onto the IP Phone.

The Pingtel SIP-based phone downloads applications from a configured location. The default applications are retrieved from http://appsrv.pingtel.com when the phone first boots. By altering the DNS settings to point to a malicious server, it is possible to cause the phone to download and install a malicious package from an alternate location. Additionally, the phone's firmware can be upgraded without administrative privileges.

VoIP Deployment Scenarios

The actual level of threat posed to an enterprise VoIP network varies based on the network's deployment configuration, several of which are discussed below.

Campus/internal VoIP

The vast majority of VoIP deployments are campus level, where IP voice is converted to TDM by a media gateway for access to the PSTN. VoIP services do not connect to the Internet or any other untrusted network. Most of these environments use switched networks and VLANs, which further segment the VoIP. In these installations, VoIP is basically an island with a TDM perimeter. Of course, the VoIP does interact with the LAN, which is connected to the Internet, so it is possible for an attacker to gain access to the LAN. Since an attack on the VoIP network must originate within the internal network, the threat is considered moderate.

Figure 8 illustrates the risks involved with a campus/internal VoIP deployment. The internal threat (i.e., an internal worker or a worker/vendor with remote access to the network) can access and exploit the IP PBXs. Toll fraud or DoS attacks may be initiated against resources outside the enterprise, creating liability and cost issues for the enterprise. The legacy voice network continues to provide remote access into the enterprise LAN, as discussed with reference to Figures 2, 3, and 4.

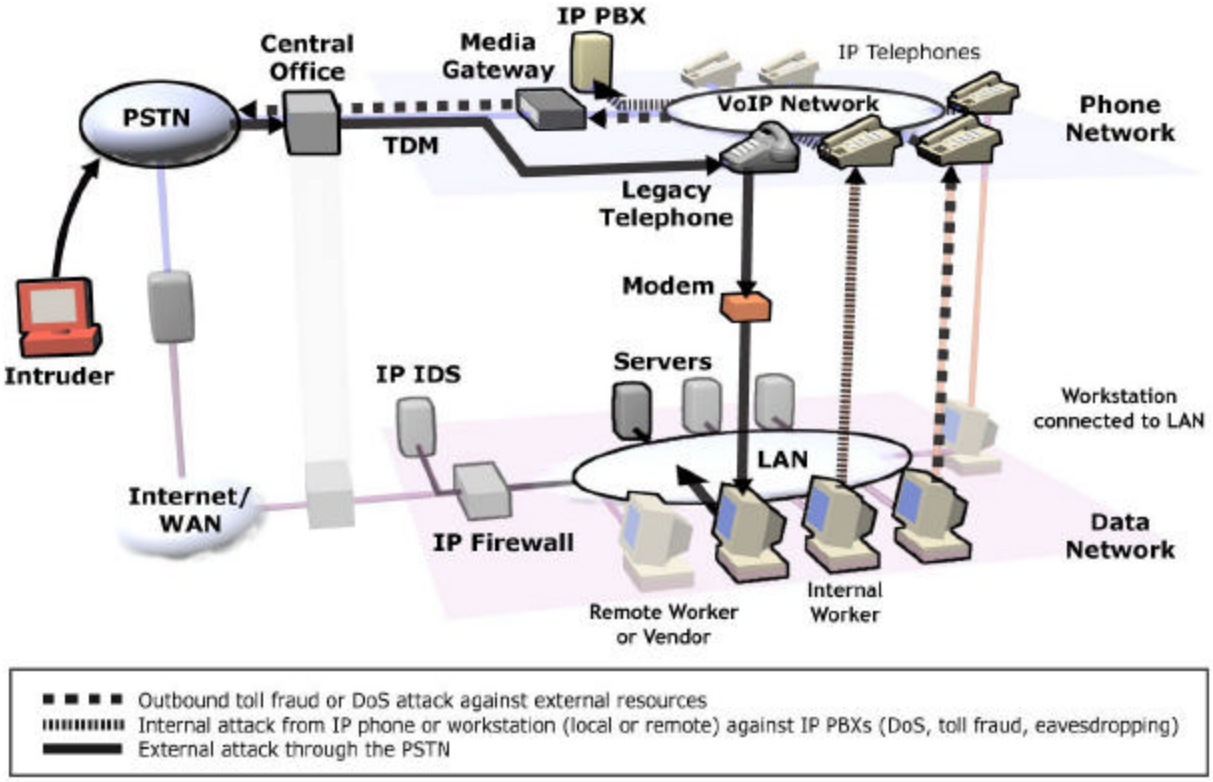

Figure 8 – Campus/Internal VoIP Risks

IP Centrex/Hosted IP

According to Frost and Sullivan, the IP Centrex market is expected to grow to 10 million lines by 2008. [11] In this scenario, the IP PBXs are located at and managed by a service provider, moving the responsibility for security to the service provider—which "should" increase security. However, VoIP must now traverse between the trusted and untrusted perimeter of the enterprise and pass through the enterprise firewall. As discussed previously, traditional data firewalls are inadequate to meet the unique real-time, reliability, security, and session management requirements of VoIP. The internal threat found in a campus deployment still exists with IP Centrex, in addition to a threat from the service provider's shared/untrusted network; therefore, the threat level is considered high.

Figure 9 illustrates the various risks associated with an IP Centrex deployment. The LAN is accessible by an attack through the service provider's shared network. Attacks launched from within the enterprise, as well those through the legacy phone network continue to be issues.

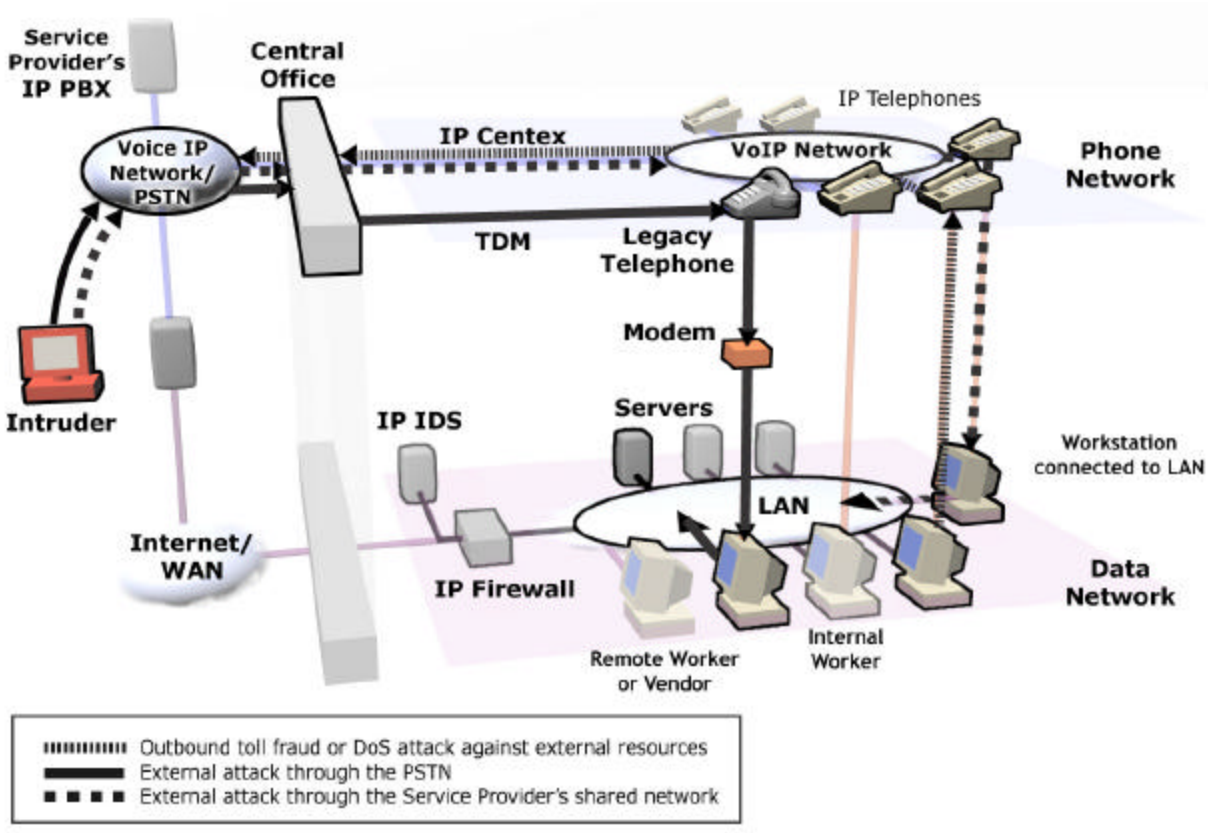

Figure 9 – IP Centrex VoIP Risks

End-to-End VoIP

Long term, VoIP calls will be transported as IP end-to-end. Service providers will manage the media gateways that translate between VoIP and legacy TDM—and TDM will be the island, rather than VoIP being the island. This deployment can offer enhanced applications and less expensive calling. Most enterprises, especially large ones, will manage their own IP PBXs and accept VoIP from an untrusted network. In an end-to-end VoIP deployment, the voice network can be attacked directly from the untrusted external voice network; therefore, the threat level is high.

Figure 10 illustrates the multiple risks presented whenever VoIP services are received from an untrusted IP network. Internal attacks against the IP PBXs, outbound attacks against external resources, and inbound attacks directly from the external voice network are all capable of exploiting vulnerabilities.

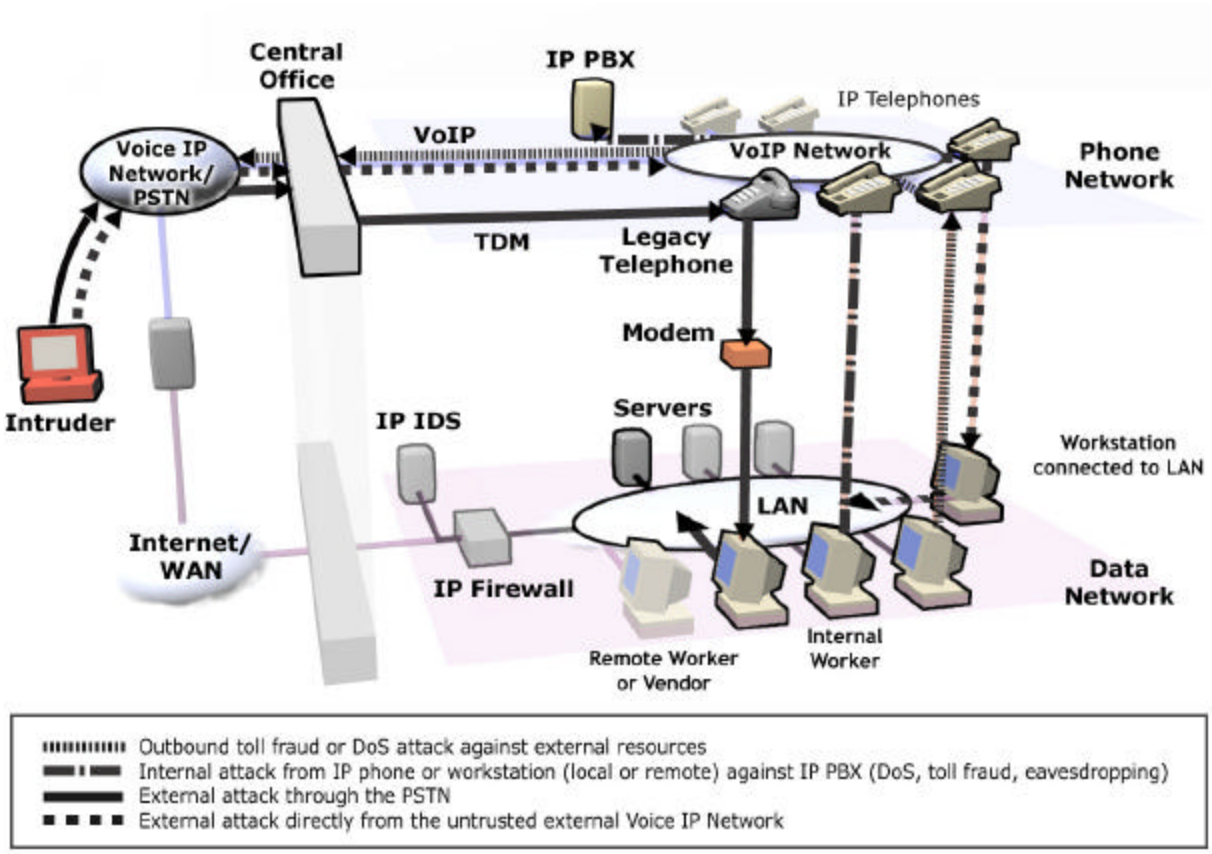

Figure 10 – End-to-End VoIP Risks

4. Hybrid Circuit-Switched/VoIP Vulnerabilities and Threats

During the transition from traditional circuit-switched voice to VoIP, most enterprises will slowly deploy VoIP technology by using a hybrid network consisting of both legacy circuit-switched and VoIP equipment. Even after an enterprise becomes "all-VoIP," is it likely that TDM-based services such as data modems, fax machines, dial-in maintenance ports, alarm systems, and backup emergency connection to the PSTN will continue to be supported in parallel with the new VoIP network. The security issues with circuit-switched networks will persist, new issues with VoIP will be introduced—and variations on the circuit-switched and VoIP issues.

5. Summary

The traditional voice network, the emerging VoIP network, and the IP data network face significant threats through the unsecured telecom environment. Unauthorized and non-secure modems create the majority of the threat from the traditional voice network. Although these issues have existed for years, they have become more acute due to the rapid growth of the Internet and the maturity of the tools used to protect the enterprise's connection to the Internet.

Threats from the traditional voice network will not disappear with VoIP implementation. Even after the migration period is over, enterprises will continue with a hybrid mix of legacy services and IP services.

VoIP is the future for voice communications. However, it is clear that the VoIP network will be less secure than the traditional voice network. These vulnerabilities include those common to any IP service, and those that are uniquely a result of the complexity and real-time requirements of the voice service.

As long as VoIP is primarily implemented as an internal service, its inherent vulnerabilities represent a risk similar to other internal IP applications. However, when the enterprise connects VoIP to the untrusted network, the threat will increase significantly—and conventional perimeter security devices are not designed to adequately support the unique requirements of voice communications.

Voice managers need to be able to control security across a mixture of both circuit-switched and VoIP networks. They need to both secure their entire voice service and adapt as their network migrates to VoIP. Voice managers need a solution that is agnostic to the underlying transport type, has a robust management infrastructure, and a user interface that insulates them from the myriad details of the underlying hardware, transport, and protocols.

Acronyms

ACD – Automatic Call Distribution
B2BUA – Back-to-Back User Agent
CDR – Call Detail Recording
CPE – Customer Premise Equipment
DISA – Direct Inward Service Access
DNS – Domain Name Server
DoS – Denial of Service
DTMF – Dual Tone Multi-Frequency
HTTP – HyperText Transfer Protocol
IDP – Intrusion Detection/Prevention
IM – Instant Messaging
IP – Internet Protocol
IPsec – IP Security
IPT – IP Telephony
ISP – Internet Service Provider
IVR – Interactive Voice Response
LAN – Local Area Network
MITM – Man-In-The-Middle
NAT – Network Address Translation
PABX – Private Automatic Branch eXchange
PBX – Public Branch eXchange
PC – Personal Computer
PDA – Personal Digital Assistant
PSTN – Public Switched Telephone Network
QoS – Quality of Service
RAS – Remote Access Servers
RTCP – Real Time Conferencing Protocol
RTP – Real-time Transport Protocol
S/MIME – Secure Multipurpose Internet Mail Extension
SCADA – Supervisory Control and Data Access
SDP – Session Description Protocol
SIP – Session Initiation Protocol
SMTP – Simple Mail Transfer Protocol
STE – Secure Telephone Equipment
STU – Secure Telephone Unit
TDM – Time Division Multiplex
TFTP – Trivial File Transfer Protocol
TLS – Transport Level Security
UA – User Agent
UDP – User Datagram Protocol
VLAN – Virtual LANs
VPN – Virtual Private Network
VoIP – Voice over Internet Protocol
WAN – Wide Area Network

References

[1] Herrell, Elizabeth, *Resolving Security Risks for IP Telephony; What Companies Need to Consider when Deploying Voice on Data Networks.* Forrester Research, Inc., August 23, 2004.

[2] Goggans, Chris, *Signal Magazine, Official Publication of AFCE*A. August 2000.

[3] Johnson, Scott, *SANS Institute Resources*. September 2000.

[4] Computer Security Institute, *1999 CSI/FBI Computer Crime and Security Survey*. 1999.

[5] *Information Security Magazine*. June 1999.

[6] Livingston, Joe, *The Desktop Modem Threat*. SANS Institute Resources, July 2000.

[7] Computer Security Institute, *2003 CSI/FBI Computer Crime and Security Survey*. 2003.
http://www.visionael.com/products/security_audit/FBI_CSI_2003.pdf

[8] Computer Security Institute, *2004 CSI/FBI Computer Crime and Security Survey*. 2004.
http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf

[9] Communications Fraud Control Association (CFCA), *Background and additional information for news writers and editors considering writing a story on CFCA's recent telecom fraud survey*. March 14, 2003.
http://www.cfca.org/Documents/fraudloss_background.pdf

[10] Gray, Patrick, *H.323 VoIP holes remain open*. ZDNET, January 16, 2004.
http://news.zdnet.com/2100-1009-5142132.html

[11] Frost and Sullivan, *U.S. Traditional and Next-Generation Centrex Services Markets*. August 2002.

13750 San Pedro, Suite 230 • San Antonio, Texas 78232 • PH: 210.402.9669 • FX: 210.402.6996 • TF: 800.817.4837
www.securelogix.com