

DTEC 6823 Term Paper

Sound Choices for VoIP Security

Jonathan Casteel

11/29/05

VoIP Security

The future of voice communications, much like most everything else, is going with some type of Internet Protocol (IP) implementation. In voice communications, this technology is called Voice over IP or VoIP. Along with any technology being implemented with data or any kind, whether it be computer data, voice information, banking information, or any other sort of information for that matter, there is always the topic of security of the technology that is a major concern. People want to feel secure and protected in everyway, and voice communications is no different. Some of the main security issues that arise with VoIP are similar if not exactly the same to issues regarding network security. Today's world rides on the backbone of the Internet, which is possible due to IP addresses. VoIP also uses IP addresses as its basis for locating other entities out there on the voice communications network. As a result, IP security is a vitally important issue to address in order to secure the VoIP network that will eventually, like the Internet is now for electronic data, be the backbone of voice communications around the world.

Many of the VoIP network security issues can be addressed by implementing existing general IP security, using this security to protect IP PBXs, engineering the network for security, implementing protection of IP phones, and implementing VoIP-optimized firewalls. In order to know where to start, understanding the vulnerabilities of VoIP is vital. At that point, a system should be put in place that follows some basic security recommendations.

As the implementation of VoIP continues to grow, many enterprises will use a hybrid network, consisting of the older circuit-switched phone system, and the newer VoIP equipment. As this architectural configuration is utilized, existing issues with the security of circuit-switched networks will continue to remain, while new security issues will surface concerning security with VoIP. Some of the circuit-switched network vulnerabilities include toll fraud, theft of service, attacks on modems, use of unauthorized modems, and eavesdropping in the PSTN (Public Switched Telephone Network). As long as circuit-switched networks are present, problems such as toll fraud and theft of service will remain to exist, and in some cases, these problems may only become more severe.

The above mentioned security issues, as well as emerging vulnerabilities that come along with VoIP will be best addressed with some type of unified security approach that will deal with both circuit-switched and VoIP security issues.

Possible VoIP deployment scenarios include:

- Campus VoIP
- IP Centrex/Hosted IP
- VoIP Trunks

Campus VoIP involves the purchase of an IP PBX, or IP-enabling an existing PBX. Implementation of an IP PBX is the most common form of deployment for VoIP.

Sound Choices for VoIP Security

Implementing an IP PBX also involves using both IP phones as well as possibly some softphones. Assuming a typical scenario, all external calls will go through a media gateway to the PSTN, therefore, VoIP does not extend to the Internet or some non-trusted network. This scenario implies that any attack on the VoIP network must originate from within the internal network, because it can not come directly from the Internet. This form of deployment is often extended to carry VoIP calls of a WAN (Wide Area Network). The implementation of carrying these calls over a WAN saves toll charges between sites. Another means of deploying campus VoIP involves extending voice services to remote workers, however, providing service in this manner increases the security threat if the remote site is not secure.

The IP Centrex/Hosted IP scenario involves a service provider managing the IP PBX and providing VoIP services from their network. No voice CPE (Customer Premise Equipment) is present, other than the IP phones. In this scenario, the threat of internal attack still exists, as well as the threat from the service provider's shared/non-trusted network.

Thirdly, let's briefly look at VoIP trunks. Over time, VoIP trunks will end up replacing the existing circuit-switched access circuits such as T1s, PRI, and analog. Additionally, voice services will come from the Internet or some non-trusted network. In this implementation scheme, the voice network is susceptible to an attack that can come directly from the non-trusted external voice network.

Some of the vulnerabilities involved with VoIP derive from the vulnerabilities that exist with regular IP networks. VoIP is a unique service that is offered on an existing IP network, and typically, the level of security of the VoIP network is only as good as the security implemented on the pre-existing IP network. Some of the security services come with the typical IP network services such as email and web services, and these services do have security vulnerabilities that are often targeted for attack. For example, VoIP services are vulnerable to viruses, worms, and Dos (Denial of Service) attacks, which have previously not been issues with the older circuit-switched networks. Another major vulnerability of VoIP networks that did not exist with circuit-switched networks is simply its susceptibility level of attack due to knowledge of attackers. In this day and age, there are many individuals with knowledge of how to attack an IP network, which in return makes VoIP networks more susceptible to attack. These attackers include individuals who know how to seek out and find vulnerabilities, how to develop exploits, and the ever growing "script kiddie" who executes attacks just for fun without really understanding the level of impact the attack may cause. VoIP, as mentioned earlier, is a service that is offered on an existing shared IP network, which makes the VoIP network accessible to users on the LAN (Local Area Network) and also, either directly or indirectly, accessible to users on the Internet.

So how do we begin to address securing a VoIP network from its vulnerabilities that we've already mentioned? Let's look at some helpful information. There are technologies that exist such as switched Ethernet and the implementation of VLANs

(Virtual Local Area Networks) that do give some defensive isolation to the VoIP network, but these are no guarantee of security. The main hope for VoIP security lies in the integration of voice communications with other applications. VoIP signaling is how services and calls are controlled, and these services are usually present on well-known IP ports. Supporting services, such as administration, which is often provided through a web server, are also implemented using well-known IP ports. VoIP requires more components and software than traditional circuit-switched networks. Some of the components include IP PBXs, supporting servers, media gateways, switches, routers, firewalls, cabling, IP phones and softphones. The area of vulnerability comes from all of these various components involved. The more components involved, the greater the potential for vulnerability. VoIP components use general-purpose operating systems. General-purpose operating systems tend to have more vulnerability issues than do proprietary operating systems built for a specific purpose. Additionally, some IP PBXs use databases and web servers that also can have vulnerabilities. There are also many so called "standards" that come along with VoIP. Some of these standards include SIP (Session Initiation Protocol), MGCP (Media Gateway Control Protocol), and vendor-proprietary protocols. There are also multiple versions of these protocols in use. Many of these standards are complex in nature and their implementations will have flaws, which leads to vulnerabilities.

Implementation flaws are programming mistakes. One example of such a mistake is not properly checking the size of a protocol request, which could result in several vulnerability points, such as:

- **Remote access** – Attackers taking control of a system via remote access, which is often an administrator level access control means.
- **Malformed request DoS** – This is a carefully crafted protocol request in the form of a packet that exploits a vulnerability which results in partial or complete loss of system function.
- **Load-based DoS** – This is a "flood" of legitimate requests that simply overwhelms a poorly designed system.

IP PBXs are the primary target for attackers due to the fact that PBXs are the primary component in providing voice service on an IP network. The software running on them can be complex and some of the vulnerabilities of the PBXs include:

- **Operating system attack** – This form of attack exploits an area of vulnerability in an operating system. An attack of such nature that may not even be directed at a VoIP network can create issues in other areas of the network.
- **Support software attack** – An attack of such nature exploits vulnerability in a key supporting software system, such as a database or web server. An example of such a situation would be an SQL Slammer worm, which exploits vulnerability in the database used on a specific IP PBX.

- **Protocol attack** – Protocol attacks can come in many varieties and forms and of course take advantage of a vulnerability in a protocol implementation
- **Application attack** – An application attack exploits vulnerability in the underlying voice application, which is not filtered by the protocol implementation.
- **Application manipulation** – This form of attack exploits a weakness in a security area, such as weak authentication or poor configuration. A weakness of such nature can allow abuse of the voice service. Some examples of this type of an attack include registration hijacking or toll fraud.
- **Unauthorized access** – The type of an attack occurs when an attacker obtains administrative access to the IP PBX.
- **Denial of Service** – This type of attack may occur by either an implementation flaw that results in loss of function or a flood of requests that overwhelms the IP PBX.

Depending on the software implementations, vulnerabilities of the natures mentioned above are also present with other components in VoIP networks.

Another serious problem is DoS on network media. The media used most commonly with VoIP is carried with RTP (Real-Time Protocol). RTP is vulnerable to an attack that is intended to congest the network or to slow the ability of the end network device to process the packets being carried in real time. Devices of such nature include a phone or network gateway. Any attacker that gains access to the segment of the network where the media is present simply needs to place a large number of RTP or high QoS (Quality of Service) packets into the network. These packets will contend with the legitimate RTP packets and cause excessive network traffic and bog down the network.

Since VoIP networks work on the backbone of a data network, some issues concerning privacy arise with users. Email messages and Instant Message sessions are typically not considered to be “private” conversations; however, voice calls are expected to be private. On a VoIP network, calls are in some cases encrypted in order to attempt to provide the privacy expected by the users, but not in all cases. Also, encryption without a strong authentication algorithm can not guarantee privacy due to the fact that participants can not be sure that an attacker is not performing a MITM (Man-In-The-Middle) attack. A MITM attack is where an attacker accesses the media within the network. If an attacker is able to gain access to the unencrypted media, all it takes are some simple tools such as VOMIT and the attacker can listen to audio.

Users expect voice calls to be private, as opposed to email or Instant Messages (IM), which are usually not expected to be private. Although some **VoIP** calls are encrypted, most are not. Additionally, encryption without strong authentication can not guarantee

privacy because participants can't be sure an attacker is not performing a Man-In-The-Middle (MITM) attack and accessing the media.

If an attacker gains access to the unencrypted media, simple tools such as VOMIT (Voice Over Misconfigured Internet Telephones) can be used to listen to audio.

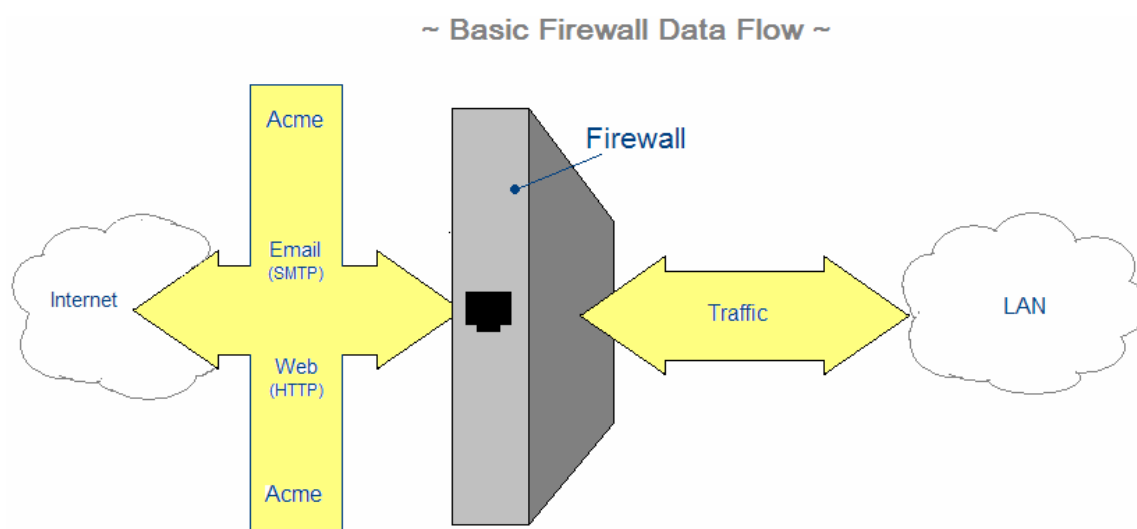
For a VoIP network environment, some of the general recommendations for implementation are listed below:

- Implement a switched network. Not only does using switches in a network improve performance, but it also makes it more difficult for an attacker to access end points.
- Within the network switches and any other applicable equipment, make use of VLANs to help segregate traffic.
- Secure all networking components, including switches, routers, etc.
- Use some form of host-based intrusion detection system to detect attacks.
- Implement a voice-optimized protection system, such as a firewall to protect the IP PBX from attackers on the LAN and Internet.
- When implementing campus VoIP, configure Internet firewalls and other security systems to prevent VoIP from entering or leaving the internal network.
- In attempts to prevent a DoS attack, limit the number of calls traveling over the WAN to the media gateway or any shared resource for that matter that could be overloaded by a DoS attack.
- Consider the implementation of additional firewalls and security products to control or monitor traffic on the network.

One of, if not the most common preventative measure taken to protect a network (data or VoIP) is to implement some sort of firewall. A firewall is either a device or piece of software that monitors network traffic between a trusted and a non-trusted network. Firewalls are placed inline at the main entrance or exit of the network framework. Since firewalls are inline, they can use rule-based policies to determine which packets to allow through the firewall and which to not allow through. A firewall may come in the form of a dedicated device, running on a device such as a router, or it could come in the form of a software package running on a computer such as a personal firewall software package. A firewall may be implemented at any location on the network, but the most common location would be at the main point where the company or organization is connected to the internet. Firewalls are implemented at a first line of defense strategy against attacks that originate from the Internet. Additionally, firewalls may be placed on a dedicated

WAN (Wide Area Network) link and also at other strategic locations inside the corporate network at a measure to protect a critical device such as an IP PBX server.

The basic principle, on which a firewall works, is it denies all access by default. If access of any kind is desired, then those services or ports have to be enabled or opened up. Rules are added to the firewall to allow certain types of TCP/IP traffic, but most all UDP traffic is denied access. The reason for this is TCP/IP traffic is viewed in general at being more secure because of its connection-oriented processes, which makes TCP/IP traffic more difficult to spoof. Types of inbound traffic is restricted to known types such as email, web access, and name service, and are only allowed to go to specific IP addresses. The outbound traffic is less restricted, but is typically confined to situations such as outbound web access to Internet web servers. Here is an illustration that displays the basic data flow for a firewall.



A firewall may also include other applications, such as a VPN (Virtual Private Network), an IDS/IPS (Intrusion Detection/Prevention System), a content filter, some sort of anti-virus software, and so on. Firewalls that are implemented at smaller-scale sites usually combine these various applications mentioned above into one single platform. On the other hand, at a larger implementation, these various applications are typically incorporated using separate platforms for more versatility and greater control of the elements involved.

Another component of firewalls that pertains to data and VoIP networks is a commonly performed function of any firewall called the NAT (Network Address Translation) service. NAT allows the use of internal private IP addresses. The use of such address scheme is needed in most cases due to the limitations in availability of public IP addresses and ports that come along with IPv4. Various types of NAT are available, and symmetric NAT is found most often in enterprises. Connections that are allowed through the firewall, the NAT service converts the internal private address/port pairs into

a separate external public address/port pair. This is very helpful in a small organizational setting that has only a single legitimate IP address and many ports. This allows the support of several connections to the Internet using only the one “real” IP address.

Within a VoIP network, the implementation of a specialized firewall would be the scenario you would find. The deployment of VoIP-optimized firewalls and security gateways at certain strategic locations in the network is recommended. Such locations would include between the IP PBX and the phones, at the WAN perimeter, and at the ISP (Internet Service Provider) perimeter. A VoIP-optimized firewall would perform the following functions:

- Provide voice application-level security by monitoring signaling for attacks. The VoIP-optimized firewall must be able to decrypt any signal that is decrypted.
- The standard for VoIP-optimized firewalls is to provide 99.999% uptime and insure that latency is not added to media sessions.
- Provides an interface with the existing data firewall where appropriate.
- The VoIP-optimized firewall should provide monitoring of the signaling and perform protocol-aware NAT and media session management.
- Preserve QoS markings.
- Interoperate with circuit-switched firewalls and to allow hybrid security during the migration period to VoIP.

Another major important aspect of VoIP to remember to make secure are the IP phones and softphones. Phones are the most common component found in a VoIP network; furthermore, they are also the easiest component of the VoIP network to exploit. Here are some of recommendations for securing the phones in a VoIP network:

- When shopping for VoIP phones, choose phones that offer strong security, such as strong authentication and/or encryption for signaling and media.
- Establish strictly governed policies regarding administrator passwords and make the standard a set of strong values.
- Configure passwords used for registration or other related functions to strong values and not simple weak “mechanical” password strings.
- Make sure any remote access features such as telnet are disabled.
- Use a strong authentication algorithm for any web-based access to the phone.

Sound Choices for VoIP Security

- Make sure local administration of the phone is disabled.
- The phone firmware upgrade process should be secured.
- If logging is an option, make sure it is enabled.
- Make the use of strong authentication for softphones a priority in order to prevent a rogue application from attacking the voice network.

On a final note, certain security standards should be implemented to allow for strong authentication and encryption. Such standards allow for interoperability between various components that are gradually being adopted by different vendors. Such standards include:

- **TLS (Transport Layer Security)** - This provides point-to-point encryption and authentication of a TCP/IP session such as that used between an IP PBX and a phone.
- **SRTP (Secure RTP)** – SRTP provides encryption of an RTP (media) session.
- **IPsec (IP Security)** – This is an OSI model Layer 3 means for encryption and authentication.
- **S/MIME** – This is used to encrypt and protect the integrity of SIP messages.

As VoIP and IP Telephony continue to mature in real-world implementations, details and new challenges as well as a rainbow of variations of challenges regarding the technology involved will continue to surface. One of the most popular conversation topics these days is in regard to security in many different areas of society, and of course, technological security is among the hottest topics of them all. In regards to the topic of VoIP security and of the vulnerabilities, both known and unknown, and all of the side effects of network intrusion attacks and denial of service attacks of such technologies, concerns are raised over the technology's vulnerabilities and we can be assured that the discussions of this topic will be in the forefront of the voice communications industry for years to come.

Sound Choices for VoIP Security

References:

Note: all of the “www.lib.co.rowan.nc.us/” links were pulled from journal samples from the Salisbury, NC Rowan Public Library NCLIVE resource site of technical journals.

<http://www.lib.co.rowan.nc.us/TELCO ACT NEEDS VoIP SECURITY.htm>

<http://www.lib.co.rowan.nc.us/TAKING THE threat OUT OF IP VOICE.htm>

<http://www.lib.co.rowan.nc.us/Snooping, Sniffing & VoIP.htm>

<http://www.lib.co.rowan.nc.us/Network Identity and VoIP Security.htm>

<http://www.lib.co.rowan.nc.us/Alliance tackles VOIP threats.htm>

<http://www.lib.co.rowan.nc.us/A VoIP security plan of attack.htm>

<http://www.lib.co.rowan.nc.us/Voice over IP finding a balance between flexible access and risk of external attack.htm>

<http://www.lib.co.rowan.nc.us/Nortel raises VoIP security flag at RSA show.htm>

<http://www.lib.co.rowan.nc.us/VoIP security concerns cannot be ignored.htm>

<http://www.lib.co.rowan.nc.us/supplier group to address voip sec concerns.htm>

<http://www.lib.co.rowan.nc.us/Meeting the Wireless VoIP Security Challenge.htm>

<http://www.lib.co.rowan.nc.us/FIGHTING BACK AGAINST THREATS TO VOICE OVER IP.htm>

<http://www.lib.co.rowan.nc.us/Industry group plans VoIP best practices.htm>

<http://www.lib.co.rowan.nc.us/VoIP Industry Moves to Bolster Network Security.htm>

<http://www.lib.co.rowan.nc.us/VoIP security vendors debut new tools.htm>

<http://www.lib.co.rowan.nc.us/VoIP security threats Fact or fiction.htm>

<http://www.lib.co.rowan.nc.us/Carriers need to get a clue on VoIP services.htm>

http://download.securelogix.com/library/voice_over_ip_firewalls_050105.pdf