Global Information Assurance Certification Paper

Security Issues and countermeasure for VoIP

GIAC Security Essentials

GIAC Gold Paper for GSEC

by
Jianqiang Xin
jqxin@eng.iastate.edu

Table of Contents

List of Figures

Abstract

Voice over Internet Protocol (VoIP) has been widely deployed since the integration of the voice and data networks reduces management effort and cost. Since VoIP share the same infrastructure with traditional data network, it inherits all security problems from data network. Furthermore, VoIP also has its own security problems coming from new protocols and network component. This paper focuses on these VoIP specific security threats and the countermeasures to mitigate the problem.

At first, this paper gives a brief introduction of VoIP techniques: the network structure, network components, protocols and standards, data handling procedures, quality of service requirements, etc. Secondly, the paper discusses the VoIP specific security threats using the principle of CIA (Confidentiality, Integrity and Availability). The countermeasure to mitigate these threats is also discussed. At last, the paper proposes some common practice to secure VoIP networks.

Document Conventions

When you read this practical assignment, you will see that certain words are represented in different fonts and typefaces. The types of words that are represented this way include the following:

Command	Operating system commands are represented in this font style. This style indicates a command that is entered at a command prompt or shell.
Filename	Filenames, paths, and directory names are represented in this style.
computer output	The results of a command and other computer output are in this style
URL	Web URL's are shown in this style.
Quotation	A citation or quotation from a book or web site is in this style.

Introduction

Voice over Internet Protocol (also called VoIP, IP telephony, Internet telephony and Digital Phone) is the routing of voice conversation over the Internet or any other IP-based network. The voice data flows over a general-purpose packet-switched network, instead of traditional dedicated circuit-switched voice transmission lines [1].

Advantages of VoIP include toll bypass, network consolidation and service convergence. Thousands of dollars are saved for large enterprises by placing long distance calls over an IP network instead of traditional telephone system. Network consolidation enables the transmission of data, voice, and video over one single network. The integration greatly reduces setup and maintenance costs. With service convergence, enhanced functionality can be implemented through coupling of multimedia services [3]. The deployment rate of VoIP is increasing steadily. According to Juniper Research, the rapid growth of the global VoIP market will contribute $18 billion in revenues by 2010 [3].

Securing VoIP system is more challenging than securing pure data network. First, all security problems related with data network appear in VoIP system since they share same network infrastructure. Secondly, VoIP does not have a dominant standard so far. The support of two standards in products just increases the chance of buggy application. Dozens of proprietary protocols make the matter worse. Thirdly, the QoS (Quality of Service) requirement of VoIP leaves less working room for possible security measures. A very secure VoIP system that can not deliver good voice quality is not attractive.

Since the security of data network is well studied so far, this paper will focus on VoIP specific security threats and their countermeasures.

Overview of VoIP techniques

Although VoIP is already widely implemented, the technology is far from mature. There is not a dominant protocol standard in the markets. Every vendor uses either its own proprietary or one of two standards, H.323 and SIP (Session Initiation Protocol). For example, Cisco uses the SCCP (Signaling Connection Control Part) protocol, Avaya uses the H.323 protocol with proprietary extensions and Nortel uses the UNISTIM (Unified Network Stimulus) protocol [2]. Proprietary protocols make it difficult to inter-connect products from different vendors. Good news is that more and more vendors begin to support H.323 or SIP.

VoIP transfer voice signal over IP based network. First, human voice needs to be converted to digital bits and encapsulated in packets, which are transmitted using IP network and converted back to voice signal at the destination. Secondly, there should be a way to identify each entity in the network like phone number in traditional telephone system. Thirdly, VoIP entities need to be able to communicate with telephones of PSTN.

VoIP components

The major components of a general VoIP network are illustrated in Figure 1. The gateway converts signals from the traditional telephony interfaces to VoIP. The server provides management and administrative functions to support the routing of calls across the network. In a system based on H.323, the server is known as a gatekeeper. In SIP system, the server is a SIP server. The IP network provides connectivity between all the terminals. It can be a private network, an Intranet, or Internet. The end user equipments are terminals that have native VoIP support and can connect directly to an IP network [3].

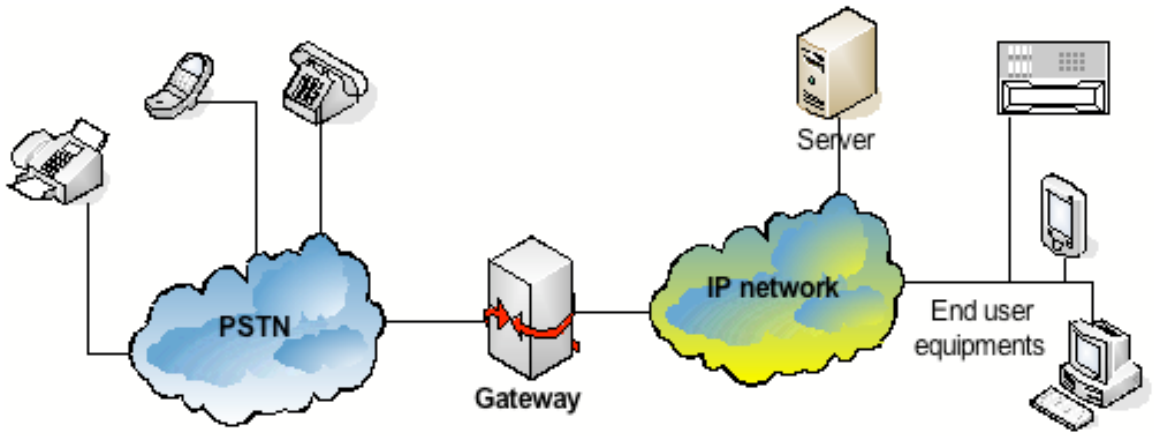

Figure 1 The major components of VoIP

The list includes several popular types of end user equipments [5]:

- Softphone or PC: With a headset, software, and inexpensive connection service, any PC or workstation can be used as a VoIP unit. Some free client software is Skype, Ekiga, GnomeMeeting, Microsoft Netmeeting, SIPSet, etc.
- Traditional telephones with adapters: traditional telephones can connect to a remote VoIP server with the aid of an analog telephone adapter or digital telephone adapter. The adapter is a device with at least one telephone jack and an Ethernet jack or a USB adapter. Some example products include AudioCodes MP-202ATA, Cisco ATA 18x Analog IP Adapter, D-Link DVG-1402s, Vtech 4106 VoIP Terminal Adapter, Nortel ATA-2 Enhanced Terminal Adapter, etc.
- IP phone: With the appearance of a conventional phone, IP phone can communicate directly with a VoIP server, VoIP gateway or another VoIP phone. The products in the market include 3Com® 3101 Basic Phone, Cisco 7961G-Ge IP phone, Linksys WIP300, Tecom Intellitouch ITC3002 phone, Dlink DPH-70, Nortel IP Phone 2001, etc.

There are two typical types of gateways in the market:

- VoIP gateways: devices that bridge conventional telephone networks and equipment to VoIP telephone networks. The commercial products include Datang MG3000-T32 Trunk Gateway, D-Link DVG-3004S, Sipura 3000, etc.
- VoIP GSM Gateway: devices that enable direct routing between IP, digital, analog and GSM networks. Here lists several commercial products: 2N VoiceBlue

Enterprise, VoIP GSM Gateway HG-4000, SIPCPE Fx-300 GSM Call Director, etc.

In Figure 2, the physical appearance of several commercial VoIP products mentioned above is illustrated. For more VoIP product information, please refer to http://www.voip-info.org/wiki/

Cisco 7961G-GE

Linksys WIP300

AudioCodes MP-202 ATA

Datang MG3000-T32 Trunk Gateway

Figure 2: VoIP Product views

VoIP Data handling

VoIP data handling has two steps: call setup and voice data processing. During call setup, the requester locates and contacts the recipient to create voice data transmission channels. For example, Alice dials an SIP address of Bob bob@example.com on her IP phone. Bob's IP address is found by proxy servers of Alice and Bob. Then, a connection is established between Alice's phone and Bob's phone so that they can negotiate necessary parameters for voice data transmission. These parameters include voice encoding codec, encryption scheme, UDP ports, etc. At last, the channels for voice data transmission are created.

Figure 3 illustrates the basic flow of voice data in a VoIP system. In the beginning, human voice must be converted into digitized form. Then, the digitized voice is compressed to save bandwidth. Optionally, encryption can also be used to protect the conversation from sniffing. Next, voice samples are inserted into data packets to be carried on IP networks. The protocol for the voice packets is typically the RTP (Real-time Transport Protocol), which is defined in FC 3550. RTP packets have special header fields that hold data needed to correctly re-assemble the packets into a voice signal on the other end. Voice packets are generally carried by UDP protocols due to its low overhead and its suitability for real-time processing. At the other end, the process is reversed: the packets are disassembled and put into the proper order; digitized voice data are extracted from the packets and uncompressed; the digitized voice is processed by a digital-to-analog

converter to render it into analog signals for the called party's handset speaker.

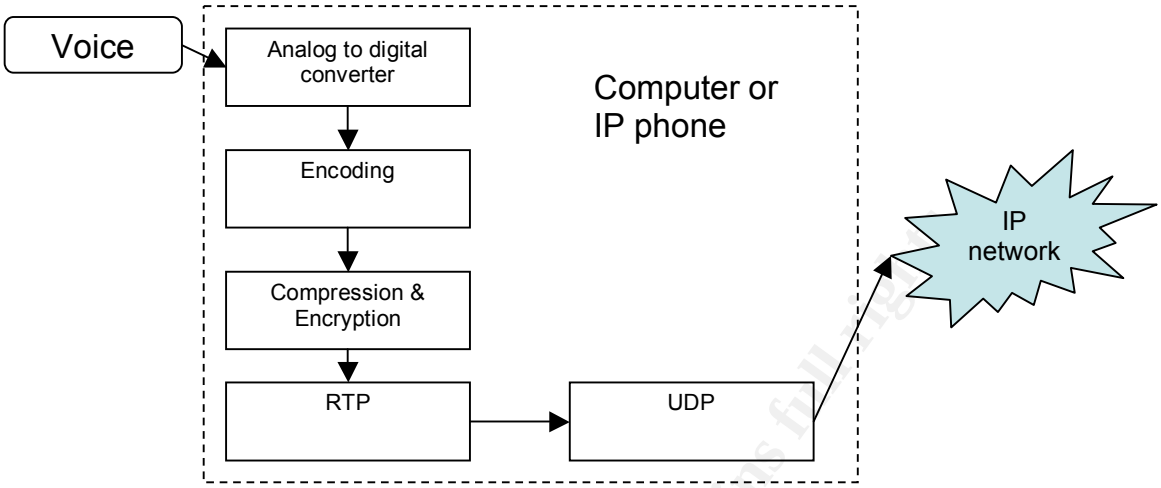

Figure 3: Voice data processing in VoIP network

Quality of Service for VoIP

Quality of Service (QoS) is vital for the success of VoIP since few will use it if VoIP can not deliver at least the same voice quality as traditional telephone network. The QoS for VoIP is mainly affected by latency, jitter (delay variation) and packet loss [6].

Latency in VoIP refers to the time it takes for a voice transmission to go from its source to its destination. The ITU-T recommendation G.114 establishes a number of time constraints on one-way latency. The upper bound for domestic calls is 150 ms for one-way traffic [10]. This time constraint limits the amount of security that can be added to a VoIP network. In the worst cases, there is only 20-50 ms left for security implementation since encoding and traveling might take 100-130ms [11,12].

Jitter refers to non-uniform packet delays. Introducing discontinuity in audio stream, jitter is more detrimental to QoS than the actual delays themselves [13]. Jitter is often caused by low bandwidth situation in VoIP.

VoIP is intolerant of packet loss. VoIP packets are very small, containing a payload of only 10-50 bytes, which is approximately 12.5-62.5ms. Therefore, occasional one packet loss is not so significant. That's one reason why VoIP packets are transmitted by UDP instead of TCP. Even with

less than 150ms of latency, a packet loss of 5% caused VoIP traffic encoded with G.711 to drop below the QoS levels of the PSTN, even with a packet loss concealment scheme [14]. "Tolerable loss rates are within 1-3% and the quality becomes intolerable when more than 3% of the voice packets are lost" [12].

VoIP protocols

VoIP needs two types of protocols: signaling protocol and media protocols. Signaling protocols manage call setup and teardown. Examples of signaling protocols include H.323, SIP, MGCP, Megaco/H.248 and other proprietary protocols like UNISTIM, SCCP, Skype, CorNet-IP, etc. Media protocols manage the transmission of voice data over IP networks. Examples of media protocols include RTP (Real-time Transport Protocol), RTCP (RTP Control Protocol), SRTP (Secure Real-time Transport Protocol) and SRTCP (Secure RTCP). A diagram of VoIP protocols is shown in Figure 5. Signaling protocols are generally transported by TCP for the benefit of reliability. Media protocols are always transmitted by UDP.

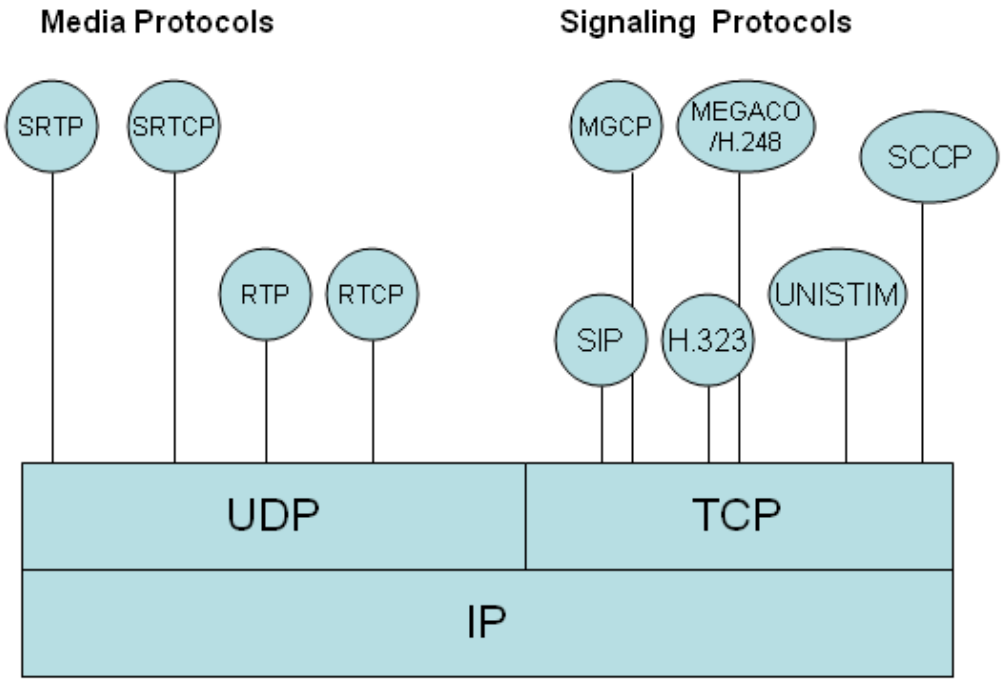

Figure 4: Diagram of VoIP protocols

H.323 protocol

H.323 was created by the ITU-T (International Telecommunication Union Telecommunication Standardization Sector). The protocol can transmit voice, video, data conference and other multimedia applications that need inter working with PSTN. H.323 is actually an umbrella standard, encompassing several other protocols like H.225, H.245, H.235 and others. Each of these protocols has a specific role in the call setup process. All protocols except H.225 use dynamic ports that need to be negotiated at previous step.

There are four types of components defined in H.323 protocol: terminals, gateways, gatekeepers and multipoint control units. Any end user equipment running H.323 protocol in Figure 1 is a terminal whether it is a PC or an IP phone. Gateways connect the H.323 network with other networks like SIP or PSTN. They translate protocols for call setup and release, convert media formats between different networks. Gatekeepers serve as the focal points within the H.323 network. The services provided by them include addressing, authorization and authentication of terminals and gateways, bandwidth management, accounting, etc. Multipoint Control Units (MCU) support conferences of three or more H.323 terminals.

Figure 5 demonstrate call setup process for H.323 protocol. Each H.323 sessions starts with address translation through a preconfigured gateway. Once the IP address of the destination is known, a TCP connection is established from the source IP to the receiver by using Q.931 protocol, which is part of H.225 protocol. During this step, both parts exchange some parameters include encoding parameters and other protocol related stuff. It also setup the address and ports used in H.245 protocol in next step. In the process of H.245 protocol, four RTCP and RTP channels are established since each channel is unidirectional. RTP channel is used to transfer voice data from one entity to another. The RTCP and RTP address and ports are also dynamically allocated in this step. Once the channels are established, the voice data are transmitted through these channels including the RTCP instructions.

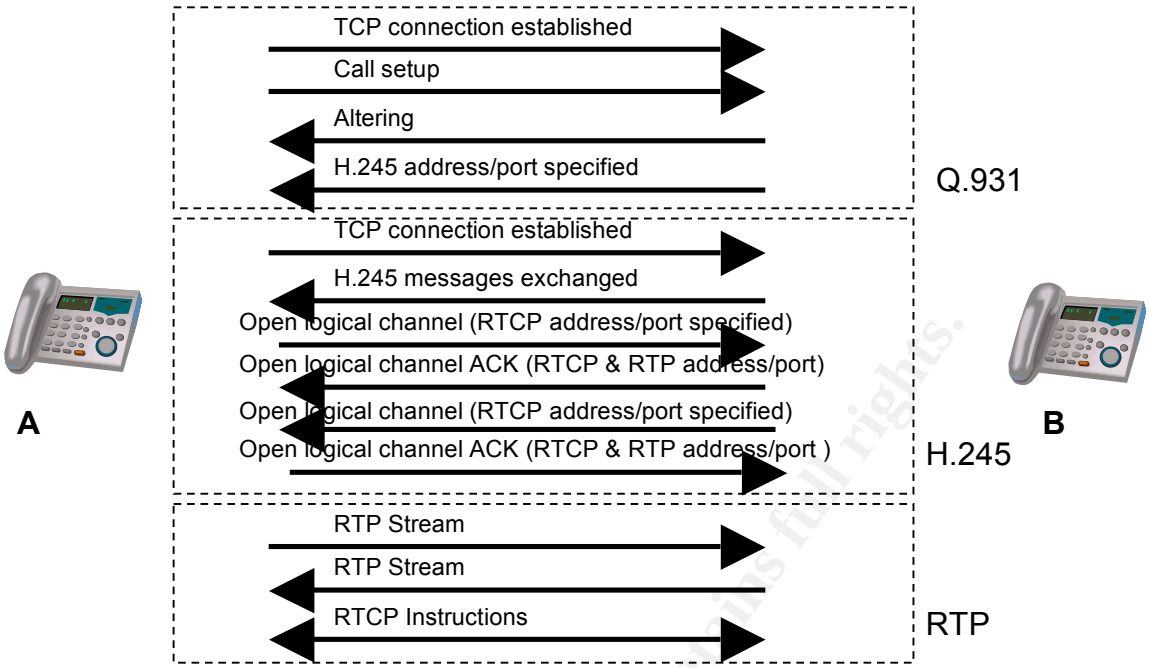

Figure 5: H.323 call setup process [6]

H.235 version 2 standard of H.323 protocol set defined different security profiles. The defined profiles provide different level of security. Baseline security profile defined in H.235v2 Annex D relies on symmetric techniques. Shared secrets are used to provide authentication and message integrity. The signature security profile of H.235v2 Annex E relies on asymmetric techniques. Certificates and digital signatures are used to provide authentication and message integrity. Hybrid security profile defined in H.235v2 Annex F relies on asymmetric and symmetric techniques. It can be seen as a combination of the baseline and the signature security profile. During the first handshake between two entities, certificates and digital signatures are used to authenticate and provide message integrity. During this handshake a shared secret is established that will be used further on in the same way described for the Baseline security profile. Voice encryption option defined in H.235v2 Annex D offers confidentiality for the voice media stream data. The supported encryption algorithms include 56-bit DES, 56-RC2, Triple-DES and AES. It can be used in combination with baseline security profile, signature security profile or hybrid signature security profile.

Session Initiation Protocol (SIP)

Session Initiation Protocol was developed by Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control (MMUSIC) Working Group in RFC 3261. This text-based protocol is considered simpler than H.323. SIP is very much like HTTP, the Web protocol, or SMTP. Messages consist of headers and a message body that defined in the Session Description Protocol (SDP). SIP is an application protocol and can be carried out by UDP, TCP and STCP protocols.

The architecture of a SIP network is different from the H.323 structure. A SIP network is made up of end points, proxy, redirect server, location server and registrar. The user needs to tell a registrar about their location. This information is subsequently saved in the external location server. SIP messages are forwarded by either proxies or redirect server. Proxy servers extract "to" information from the message and contact the corresponding location server and forward the packets to the end machines or related servers. Redirect server, on the contrary, just send back the information to the original sender.

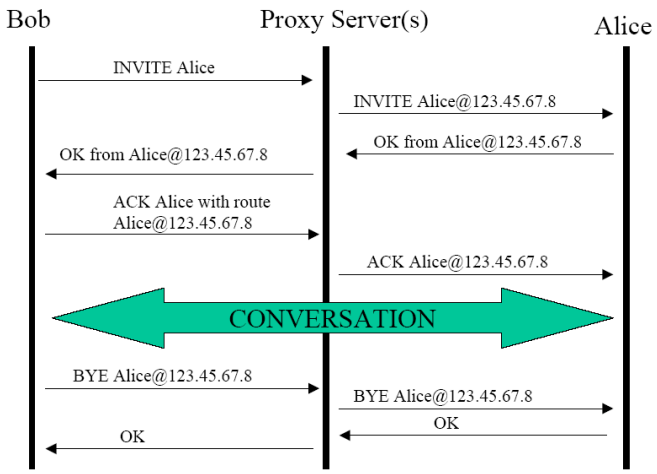

Figure 6: SIP protocol [6]

The SIP protocol is modeled on the three way handshake method of TCP. In Figure 6, an example with a proxy and two endpoints is shown. Session Description Protocol (SDP) is used here to include fields for the codec used, caller's name, etc. In the figure, Bob sends an INVITE request to the proxy server with SDP information. The proxy server forward Bob's request to Alice's client. If Alice wants to accept the call from Bob, she will send an "OK" message back containing her call preference in SDP format. Then Bob

responds with an "ACK". After the "ACK" is received, the conversion may start along with the RTP/RTCP agreed upon in previous steps. When the conversion is over, Bob send and "BYE" message and Alice reply with an "OK" message.

Unlike H.323, SIP does not define its own security profile. SIP can use HTTP digest authentication, TLS, IPSec and S/MIME (Secure/Multipurpose Internet Mail Extension) for security.

MGCP and Megaco/H.248

Media Gateway Control Protocols (MGCP) is used to communicate between the separate components of a decomposed VoIP gateway. It is a complementary protocol to SIP and H.323. Within MGCP the MGC server is mandatory and manages calls and conferences and supports the services provided. The MG endpoint is unaware of the calls and conferences. MGCP is a master/slave protocol with a tight coupling between the MG (endpoint) and MGC (server).

MEGACO/H.248 is derived from MGCP and is expected to be accepted widely in the industry. The improvements of MEGACO/H.248 include support of multimedia and multipoint conferencing enhanced services, improved syntax for more efficient semantic messages processing, allowing either text or binary encoding and expanded definition of packages. Megaco recommends security mechanisms that may be in underlying transport mechanisms, such as IPSec. H.248 requires that implementation of the H.248 protocol implement IPSec if the underlying operating system and the transport network support IPSec.

Security threats of VoIP

This section discusses various threats to confidentiality, integrity and availability of VoIP systems. Possible mitigation measures for these threats are also investigated. At last, firewall and NAT challenges are analyzed.

Confidentiality threats

Confidentiality means *that the information can not be accessed by unauthorized parties*. The confidential information of end users includes private documentation, financial information, security information like password, conversion content, conversion history or pattern, etc. The confidential information for network components includes operation systems, IP addresses, protocols used, address mapping, user records, etc. Leak of this information might make attackers' jobs easier.

Eavesdropping of phone conversation

Conventional telephone eavesdropping requires either physical access to tap a line, or penetration of a switch. With VoIP, opportunities for eavesdroppers increase dramatically because of the large number of nodes in the path between two conservation entities. If the attacker compromises any of theses nodes, he can access the IP packets flowing through that node. There are many free network analyzers and packet capture tools that can convert VoIP traffic to wave files [16]. Theses tools allow the attackers to save the conversation into the files and play them back on a computer. VoMIT (Voice over Misconfigured Internet Telephones) is an example of such a tool [17]. Ethreal can also be used to record SIP packets and retrieve voice message in wav file format.

Unauthorized access attack

Unauthorized access means that the attacker(s) can access resources on a network that they do not have the authority. Shawn Merdinger reported multiple undocumented ports and services in certain VoIP phones [18]. There are also vulnerabilities due to implementation issues [19].

There are systems for call control, administration, billing and other voice telephone functions. Repositories in these systems may contain passwords, user identities, phone numbers, and private personal information. Lots of gateways and switches are shipped with default well-known passwords. If these passwords are left without changes, the attackers can easily break in. Some switches still use TELNET for remote access. The clear-text protocol exposes everything to anyone who can sniff the network traffic. Some of the gateways or switches might have a web server interfaces for remote control. The attacker might sniff the HTTP traffic in local network to steal sensitive information. Attackers can also use ARP cache poisoning to forward all traffic through their machines to capture network traffic.

Countermeasures

Encryption of voice message packets can protect against eavesdropping. IPSec can be deployed to encrypt whole packets. SRTP can provide confidentiality, message authentication and replay protection for audio and video streams.

To better protect gateways and switches, they should use SSH instead of other clear-text protocols as remote access protocol. If web-based interface is provided, HTTPS should replace HTTP. In addition, all default passwords should be changed before the system is plugged into the network. A up-to-date intrusion detection system might detect ARP poisoning and other types of attacks.

Integrity Threats

Integrity of information means that *information remains unaltered by unauthorized users*. A legitimate user may perform an incorrect or unauthorized operations function and may cause delirious modification, destruction, deletion or disclosure of switch software and data. An intruder may masquerade as a legitimate user and access an operation port of the switch.

Caller Identification spoofing

Caller ID (Caller Identification) is usually a service provided by most telephone companies that tell users the phone number of an incoming call. Caller Identification spoofing is setting the Caller ID on the outgoing calls to a 10 digit number of the caller's choice. Several websites provide Caller ID spoofing service eliminating the need for any special hardware. The list includes www.spooftel.com, www.telespoof.com, www.callnotes.net, www.spoofcard.com, etc.

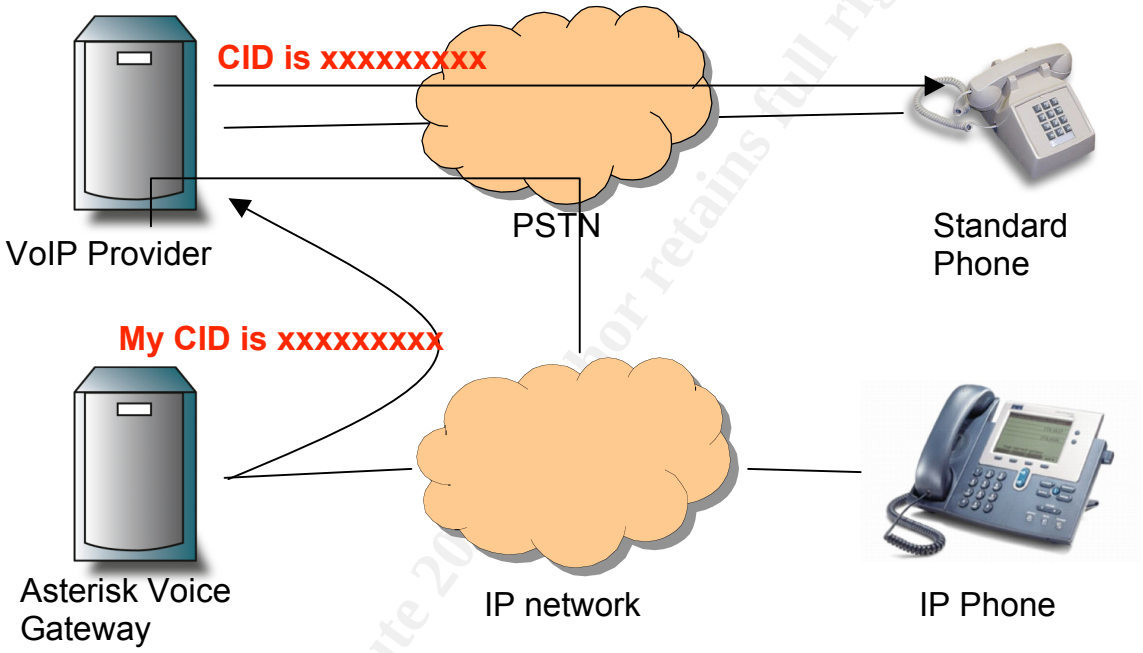

Figure 7: Illustration of Caller ID spoofing

For VoIP, Caller ID spoofing is simpler than traditional telephone as illustrated in Figure 7. Suppose Alice sent an "INVITE" message to Bob and the message is like the following (the SDP of Alice is not shown here):

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE
Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp
Content-Length: 142
```

The caller ID service relies on the "From" header to supply the identity. Call-ID contains a globally unique identifier for this call and has nothing to do with Caller ID. If the attacker can control the gateway server, he can arbitrarily

change "From" header to anything that he wants. The recipient will send back acknowledgment to this proxy server, which is the same as "via" field. The proxy server can then forward the acknowledgment to Alice since it knows the real IP address of Alice's phone. The popular proxy server software Asterisk is open source and very flexible to customize. This only makes things worse.

Automated or manual caller ID verification systems such as used by credit card companies can be sent false information. *Lance James, chief scientist at security company Secure Science Corp., said Caller ID spoofing Web sites are used by people who buy stolen credit card numbers. They will call a service such as Western Union, setting Caller ID to appear to originate from the card holder's home, and use the credit card number to order cash transfers that they then pick up* [22]. Spammers can use this feature to spam or run phishing attacks posing as banks or other trusted parties.

Registration hijacking

Registration hijacking happens when an attacker replace the legitimate registration of the victim with his address. The attack causes all incoming calls for the victim to be sent to the attacker's address.

Registration is normally performed using UDP, which make it easy to spoof registration requests. For example, Alice wants to register her address at registrar using SIP protocol. The "REGISTER" message looks like the following:

```
REGISTER sip:alice@atlanta.com SIP/2.0
Via: SIP/2.0/UDP 192.168.2.10;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Alice <sip:alice@atlanta.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@192.168.2.3
CSeq: 314159 INVITE
Contact: Alice <sip:alice@192.168.1.11:5061>;expire=60
Content-Type: application/sdp
Content-Length: 142
```

In this message, the "To" and "From" fields use the same user information. The "contact" field contains a SIP URI that represents a direct route to the device. In this example, it is IP address 192.168.1.11 and the port is 5061. "expires=60" means that the registration will expire

in 60 seconds. Another REGISTER request should be sent to refresh the user's registration.

The attacker can construct a similar REGISTER message with modified "contact" header. A possible example is like this message:

```
REGISTER sip:alice@atlanta.com SIP/2.0
Via: SIP/2.0/UDP 192.168.2.10;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Alice <sip:alice@atlanta.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@192.168.2.3
CSeq: 314159 INVITE
Contact: Alice <sip:alice@192.168.1.22:5061>;expire=60
Content-Type: application/sdp
Content-Length: 142
```

In this example, the registered IP address for Alice is changed to from 192.168.1.11 to 192.168.1.22. Fearing the victim's legitimate register requests might replace his registration, the attacker can use denial of service attack to disable the victim. The attacker can also send spoofed requests at a higher frequency than the victim.

Proxy Impersonation

Proxy impersonation attack tricks the victim into communicating with a rogue proxy set up by the attacker. Once an attacker impersonates a proxy, he has complete control of the call. Figure 8 illustrates proxy impersonation.

The attacker tricks Alice to communicate with the rogue proxy server instead of the legitimate proxy server. The UAs and proxies normally communicate using UDP and do not require strong authentication to communicate with another proxy. The attack can work by several means, including DNS (Domain Name Service) spoofing, ARP (Address Resolution Protocol) cache spoofing, DHCP spoofing, or changing proxy address for a SIP phone.

Call redirection or hijacking

Call redirection *occurs when a call is intercepted and rerouted through a different path before reaching the destination*. Possible methods include proxy impersonation and registration spoofing. The attacker can also spoof the response from the recipient and trick the requestor to talk with the attacker.

In this example, Alice wants to talk with Bob about some business secrets, which interests Tim. Tim is in the same LAN with Alice. The man-in-the-middle attack by Tim follows the below steps:

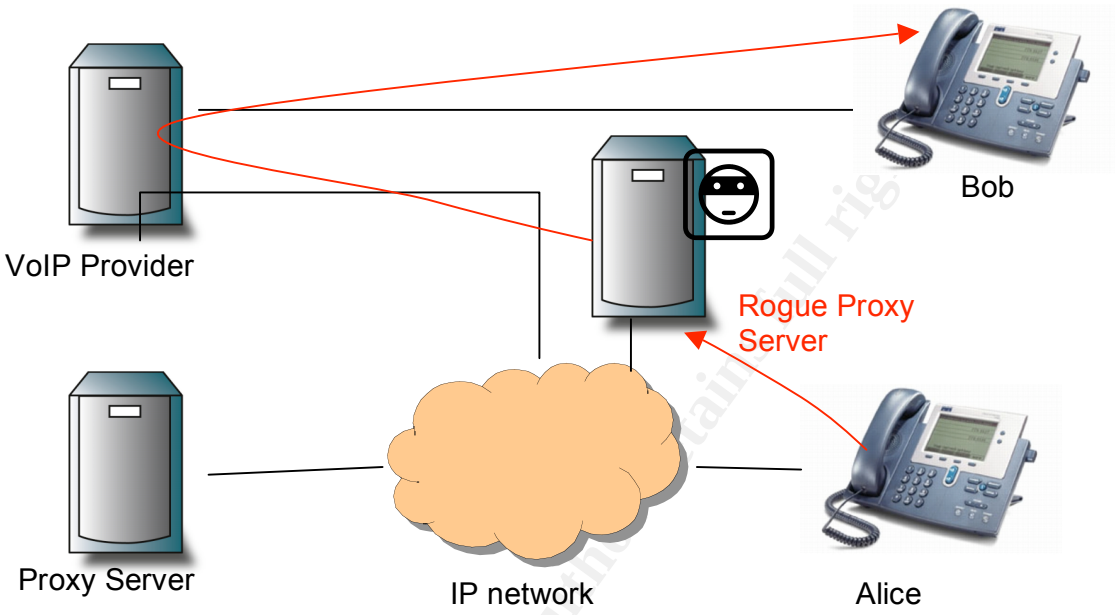

Figure 8: Illustration of Proxy Impersonation attack

1. Alice sends an Invite message to Bob and this message is detected by Tim.
2. Tim sends a response message to Alice spoofing from Bob with 301 Moved Permanently code. In the response, Tim set the new address of Alice to his computer.
3. Alice sends a new Invite message to Tim in belief that she is connecting to Bob
4. Tim sends back an Acknowledgement to establish the connection between him and Alice
5. At the same time, Tim sends an Invite message to Bob and he can also fake the caller ID of Alice.
6. Tim replies with a 200 OK and the connections between Bob and Tim is established.

Tim can use specific software to forward voice messages between two connections. He can also record the conversion contents. This is a man-in-the-middle attack. Even encryption is deployed in both connections; Tim can still access whole conversation.

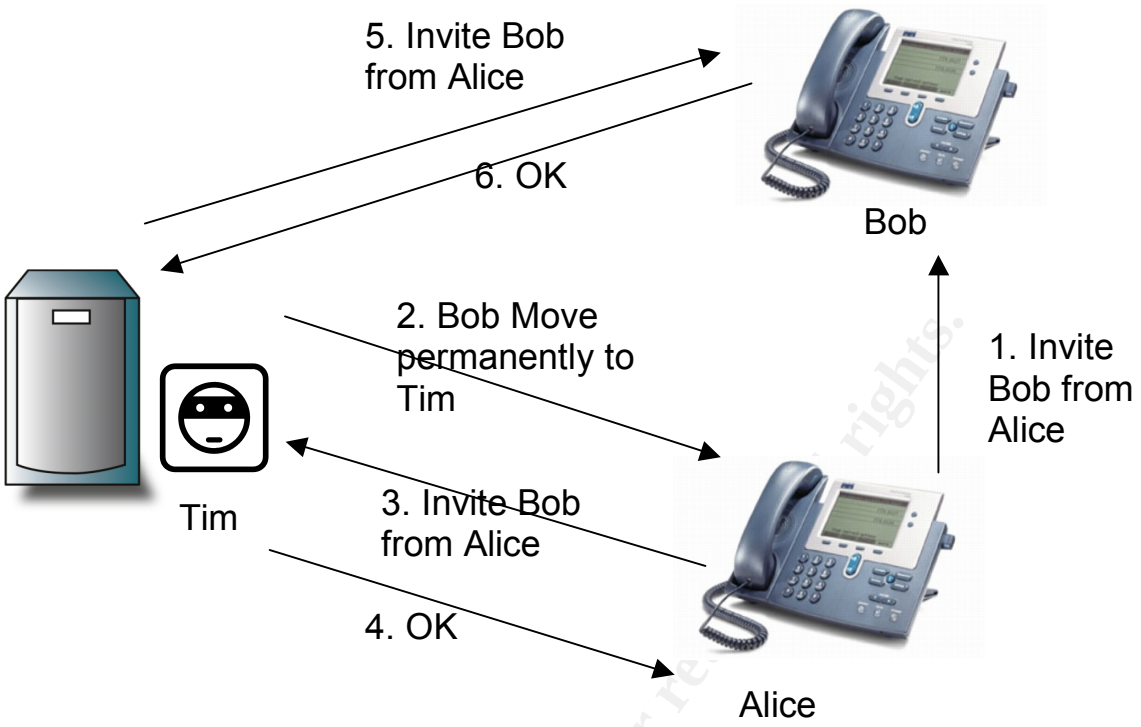

Figure 9: Illustration of Man-in-middle attack using spoof response

Call redirection or hijacking enables the attacker to eardrop even encrypted voice conversation. The attacker also can tamper the voice message sent both ways. They can also carry out replay attacks.

Countermeasures

Unfortunately, there is no effective way to prevent caller ID spoofing. The best solution so far is not to trust caller ID at all.

Stronger authentication schemes are the solutions to registration spoofing, proxy impersonating and call hijacking. To mitigate this type of attacks, software patching is crucial to fix any known vulnerabilities. VoIP vulnerability scanning tools like Sivus is strongly suggested [21].

Availability threats

Availability refers to the notion that information and services are available for use when needed. VoIP network is susceptible to denial of service attacks since DoS attacks can degrade QoS quickly to unacceptable level. Traditional DoS attacks against data networks are still very dangerous. However our focus is about VoIP specifics DoS attacks.

VoIP Signaling DoS Attacks

The attackers can abuse signaling protocol to conduct denial of service attacks. In first case, the attackers can create large number of call setup requests that consume the processing power of proxy server or terminal. One example is shown in Figure 10(a) where Tim sends way too many "invite" requests to Bob and Bob can not take request from Alice. This type of DoS attack does not have same LAN requirement. It only needs large volumes of requests to flood the victim. The attackers can also launch distributed DoS to cover trace and aggregate requests.

In the second case, the attackers use cancellation of pending call set up signals including sending a CANCEL, GOODBYE or PORT UNREQACHABLE message. This causes the phone not being able to complete calls or hang up. This type of attacks is aided by the complexity of the signal protocols. University of Oulu in Finland has developed simple SIP and H.323 protocol test suites and run them against several implementations. The results were "alarming", indicating that virtually all of the testbed components failed [20]. Figure 10(b) shows an example where CANCEL message is spoofed by the attacker to prevent call setup. Figure 10(c) gives an example where spoofed GOODBYE message tear down the established connections. One correctly crafted packet can tear down the call. However, this attack does require the attacker to be able to fill certain headers of the message correctly. The attacker can gather network data to extract this information.

VoIP Media DoS Attacks

Attackers can flood gateway, IP phone and other media-processing VoIP components with large number of RTP packets. If the target is forced to drop RTP packets, the voice quality will degrade. Furthermore, the attacker might

knock key components like gateway offline. A failure in one of these devices could bring the entire voice network to a halt. Since RTP is encapsulated in UDP, it is easy to craft.

Physical DoS Attacks

These attacks include power outrage and physical damage to network components. Traditional telephone operate on 48 volts supplied by the telephone line itself and can operate smoothly during a power failure. VoIP can not operate without power supply. Also, an attacker with physical access to any key components of VoIP network can disrupt its normal operations easily. He can plug out the power cord or network cable.

Countermeasures

To mitigate VoIP signaling and media DoS attacks, strong authentication is the key. VoIP components need to make sure that they are communicating with legitimate counterparts. VoIP firewall should also be implemented to monitor streams and filter out abnormal signals and RTP packets. Media and signal rate limits can be set by observing normal traffic patterns.

To mitigate physical DoS attacks, strict physical security schemes should be implemented with restricted areas, access control, locks, guard, etc. To guarantee continuous power supply, backup power generation system should be available.

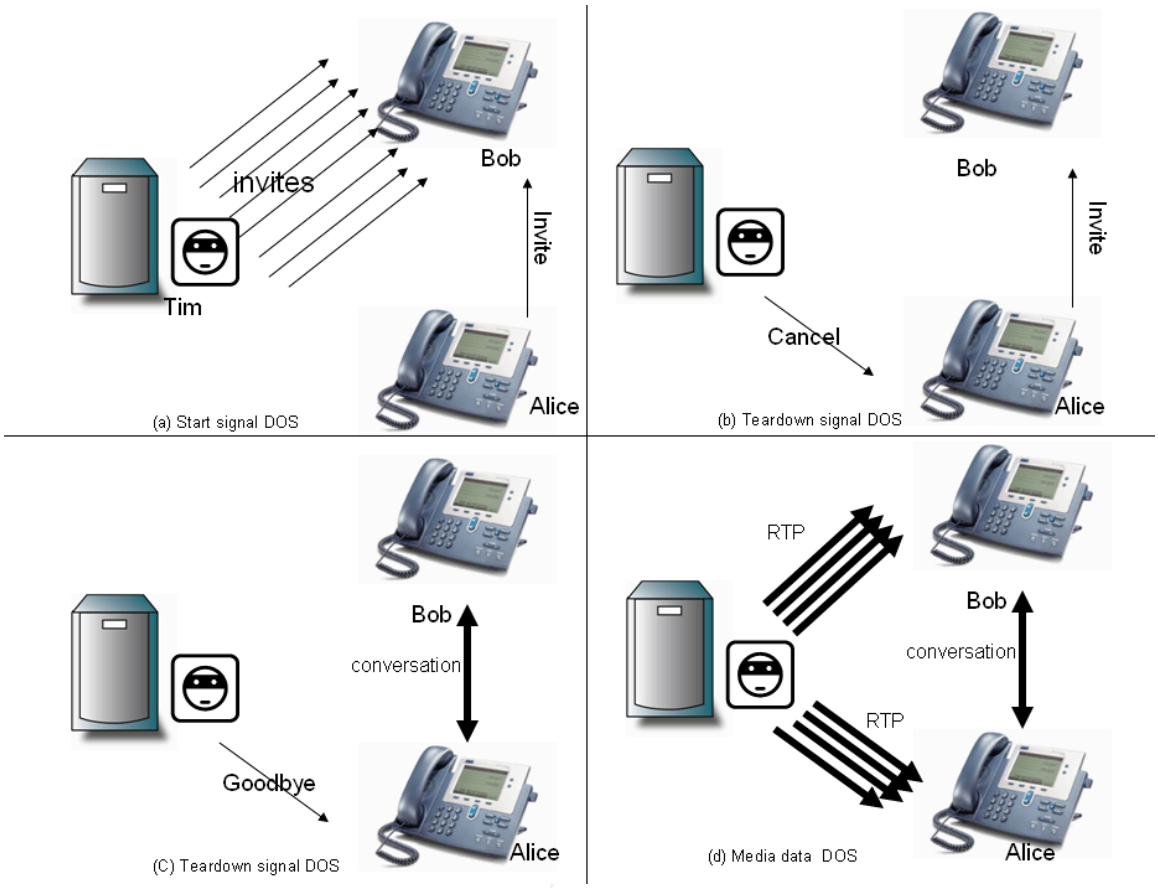

Figure 10: Illustration of VoIP specific DoS attacks

Firewall and Network Address Translation challenges

Firewalls and Network Address Translation (NAT) present a formidable challenge to VoIP implementers.

Firewalls work by blocking traffic deemed to be invasive, intrusive, or just plain malicious from flowing through them. It provides a central location for deploying security policies. The dynamic port trafficking and call setup procedures of H.323 and SIP protocol make traditional firewalls unworkable. Traditional firewalls

Network Address Translation (NAT) is a powerful tool that can be used to hide internal network addresses and enable server endpoints within a LAN to share the same external IP address. NATs also indirectly contributes to the security of the LAN, making internal IP addresses less accessible from the public Internet. NAT has significant implications for VoIP. For one thing, an attempt to make a call into the

network becomes very complex when a NAT is present. The scenario is shown in Figure 11. When Alice tried to call Bob whose internal IP address is 192.168.1.3, she only knows Bob's public IP address: 129.168.0.3. There is no way to tell whether the call is for Bob or Tim. One possible solution is to assign a static port for each internal IP address. Say Bob's address is 129.186.0.3:5611 and Tim's address is 129.186.0.3:5612. However, dynamic port allocation for voice data communication in H.323 and SIP deems this approach can not work.

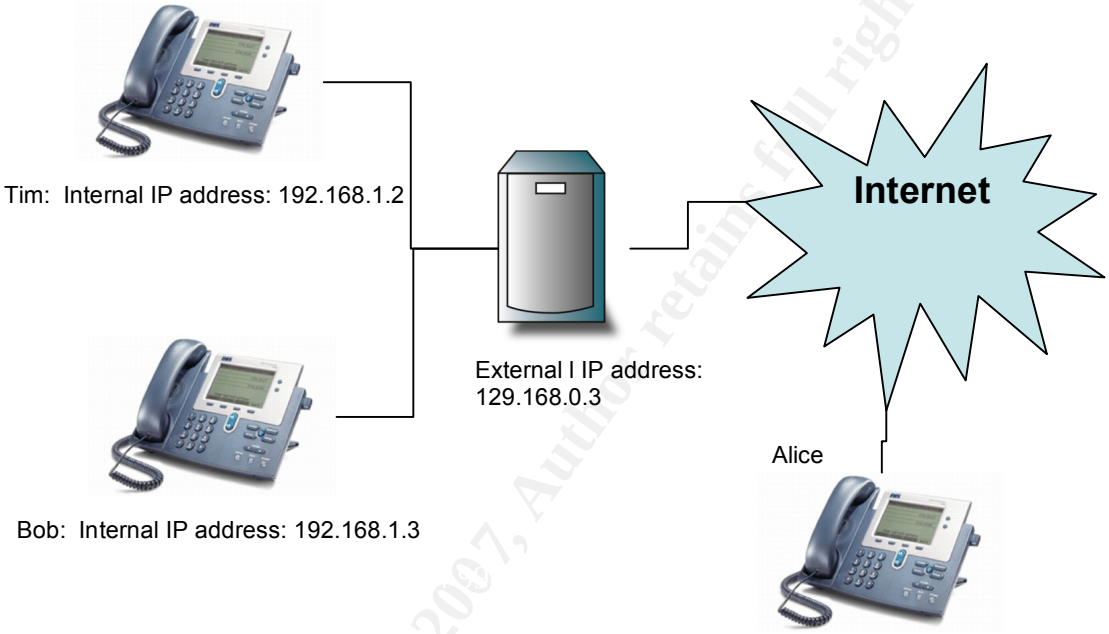

Figure 11: Illustration of NAT incoming call problems

One typical commercial solution to the firewall and NAT problem is ALGs (Application Level Gateways). "An ALG is embedded software on a firewall or NAT, that allow for dynamic configuration based on application specific information. [6]" A firewall with VoIP ALG can understand H.323 or SIP protocol so that it can open dynamic ports whenever necessary. A NAT with VoIP ALG can open up VOIP packets and re-configure internal IP address or public IP address [6].

Security Guidelines for VoIP

The introduction of voice onto corporate networks increases security risks. The good news is that there are a number of security measures that can minimize the risk of attack on VoIP systems. The following provides a list of cardinal security rules:

1. *Develop appropriate network architecture*

It is a good practice to separate voice and data on logically different networks if feasible due to their different QoS requirements. 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
A mechanism to allow VoIP traffic through firewalls
Stateful packet filters can track the state of connections, denying packets that are not part of a properly originated call. USE IPsec or Secure Shell (SSH) for remote management and auditing access. If performance is a problem, use encryption at the router or gateway, to provide IPsec tunneling [6].

2. *VoIP-ready firewalls and other appropriate protection mechanisms should be employed.*

Because of the inherent vulnerabilities of operating telephony across a packet network, VoIP systems incorporate an array of security features and protocols. "Defense in depth". VoIP-ready firewalls are essential components in the VoIP network and should be used. If permitted, state-of-the-art intrusion detection and prevention systems should also be installed.

3. *Do not use Softphone system*

In practical, "softphone" system, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern. Worms, viruses and other malicious software are extraordinarily common on PCs connected to the internet and very difficult to defend against. 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).

4. Tighten physical security control

Unless the VoIP network is encrypted, anyone with physical access to the office LAN could potentially tap into telephone conversions. Even if encryption is used, physical access to VoIP servers and gateways may allow an attacker to do traffic analysis or compromise the systems. Adequate physical security should be in place to restrict access to VoIP components.

5. Implement power back up system

Sufficient backup power should be available for the office VoIP switch, desktop instrument. There should be enough electrical power to maintain UPS battery charge. Backup power system should be periodically checked to make sure that they are ready when power is out.

6. Maintain current patch levels

Vulnerability in the operation system, software, and servers are the targets of attackers. Patching all the systems in the network is not easy.

7. Install anti-virus system and update it regularly

Viruses and worms are still the top concerns for computer security. The viruses might break down the system and disable the service.

8. Apply encryption selectively

Encryption is necessary to defeat eavesdropping attack. Transport layer security and IPsec are two main encryption methods. TLS is an alternative to IPsec and is based off the SSL protocol. Many different algorithms can be used such as DES, 3DES, AES, RC4 and RC5. The simpler encryption results in better performance.

Conclusion

In conclusion, VoIP have to deal with all security problems of traditional data network new security problem caused by new protocols and components. Quality of service requirement of VoIP limits processing time of packets by security measures. To make thing even worse, there is not one dominant protocol yet and current standards like H.323 and SIP are too complex.

Compared with traditional telephone system, it is easier to eardrop phone conversation at one of many hops in the path. Proper encryption is necessary to protect the confidentiality. Since local gateways of VoIP is very configurable, it is easier to spoof caller identities for fraudulent purposes. The best way to defense this is to remove caller ID from authentication scheme. Attacker can also hijack calls by spoofing registration, impersonating proxies or spoofing redirection response. Once the calls are hijacked, the attackers can eardrop or modify the conversation even encryption is deployed. The mitigation approach is to deploy stronger authentication measure like TLS. The attacker can also launch denial of service attacks against the shared network. They can send large number of spoof packets for call setup, call teardown to disrupt normal signaling process. They can also send large number of media packets like RTP packets. Correct deployment of firewall and IPS systems are possible mitigation measures.

It is a good practice to separate data network and voice network into two logical networks in network design. VoIP specific firewalls should be deployed in voice network to prevent malicious data traffic or voice traffic enter the system. Strong authentication and encryption should be implemented among components of VoIP for prevention of call hijacking. Power backup plan and implementation should also be examined carefully. "defense in depth" is a good principle in defending VoIP.

References

1. http://en.wikipedia.org/wiki/VoIP
2. Mark Collier, "The Current State of VoIP Security", http://download.securelogix.com/library/The_Current_State_of_VoIP_Security.pdf
3. Spirent Communications, Inc., Voice over IP (VoIP), http://www.spirentcom.com/documents/100.pdf
4. juniper research, "VoIP Services ... Deep Impact", 2006,http://www.juniperresearch.com/pdfs/whitepaper_gvoip_hnh.pdf
5. http://www.voip-info.org/wiki/
6. D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, Security Considerations for Voice Over IP Systems, Computer Security Division Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930, January 2005
7. Debashish Mitra, Network Convergence and Voice over IP, March 2001, Tata Consultancy Services, http://www.tcs.com/0_whitepapers/htdocs/voip.pdf
8. P. Mehta and S. Udani, "Overview of Voice over IP", Technical Report MS-CIS-01-31, Department of Computer Information Science, University of Pennsylvania, February 2001.
9. B. Goode, "Voice Over Internet Protocol (VoIP)", Proceedings of thee IEEE, VOL. 90, NO. 9, Sept. 2002.
10. International Telecommunications Union. ITU-T Recommendation G.114 (1998): "Delay".
11. R. Barbieri, D. Bruschi, E Rosti, "Voice over IPsec: Analysis and Solutions". Proceedings of the 18th Annual Computer Security Applications Conference,2002.
12. C-N. Chuah, "Providing End-to-End QoS for IP based Latency sensitive Applications.". Technical Report, Dept. of Electrical Engineering and Computer Science, University of California at Berkeley, 2000.
13. Anonymous, "Voice Over IP Via Virtual Private Networks: An Overview". White Paper, AVAYA Communication, Feb. 2001.
14. R. Sinden, "Comparison of Voice over IP with circuit switching techniques". Department of electronics and Computer Science, Southampton University, UK, Jan. 2002.
15. http://www.skype.com/helloagain.html

16. Roberts, C., Voice over IP security, Center for critical Infrastructure Protection, 2005.
17. Provos, N., VOMIT - Voice Over Misconfigured Internet Telephones, http://vomit.xtdnet.nl/, 2006
18. Shawn Merdinger, ACT P202S VoIP wireless phone multiple undocumented ports/services, http://www.security.nnov.ru/Ldocument66.html
19. Michael Hall, Cisco Patches VoIP Phone Vulnerability, http://www.enterprisenetworkingplanet.com/netsecur/article.php/3507801
20. Mark Collier, Voice Over IP (VoIP) Denial of Service (DoS), http://download.securelogix.com/library/DoS.pdf
21. SiVus (SiP Vulnerability Scanner) User Guide V1.07, http://www.vopsecurity.org/SiVuS-User-Doc.pdf
22. http://www.schneier.com/blog/archives/2006/03/caller_id_spoof.html