Global Information Assurance Certification Paper

SIP Deployment 101 GSEC v.1.4b

Paul Ingram

July 2003

Introduction

As more companies move to a converged network it will be doubly important to know how voice is carried on a network and how to secure it. This paper will attempt to give a brief overview of what Voice over Internet Protocol (IP) is and the security consideration for a Voice over IP (VoIP) deployment. The goal of this paper is not to be an exhaustive resource, but to highlight five areas in a Session Initiation Protocol (SIP) network and to stimulate the thought process of others as they design and deploy their own converged networks.

We will first touch on what VoIP is and some of its protocols. Secondly we will cover securing of the Proxy server by ensuring the installation is not compromised and ways of protecting the Proxy server from attacks. Thirdly we will discuss the security of the wire itself and how to fight against the man-in-the-middle (MitM) attacks by using Virtual Local Area Networks (VLAN) segmentation of voice and data traffic. Fourthly we will take a look at the security features SIP has to offer for call confidentiality. Finally I will touch on the use of Virtual Private Networks (VPN) for site-to-site security. Just as with any network, the security of your VoIP deployment lies in understanding how someone can compromise you and defending against that with a multi-layered defense.

What is Voice over IP (VoIP)?

Voice over IP is where the IP protocol is used to transport voice traffic. VoIP is quite different from switched circuit telephony. In a traditional switched circuit environment Time Division Multiplexing (TDM) is used for signal transmission. A single pair line is dropped at each handset location which is trunked back to a Private Branch Exchange (PBX). This line would then be dedicated for either an analog or digital transmission requiring a second drop of CAT5 for any Local Area Network (LAN) connections. In contrast, the VoIP technology that was first tried in the late 60's and then evolved in the 90's into its current state, sends voice traffic over an IP based network. In this manner voice and data share the same physical media and some protocol characteristics. VoIP can be thought of as any other packets traveling on the LAN segment. It is worth noting here that VoIP does have certain requirements that are not normally present in data traffic. Some of these would be the need for Quality of Services (QoS). This helps in prioritizing voice traffic over data. By doing this, latency and jitter are reduced, further enhancing the quality of the voice transmission.

Why VoIP?

Many companies deploy VoIP solely to achieve toll bypass at first. This alone can save companies thousands of dollars by reducing long distance cost for inter-office and out-office calls. Also many times businesses can save by reducing staff or eliminating maintenance contracts for PBX systems. By doing this the existing IT staff manages the converged network further reducing overhead. Also by deploying a single Wide Area Network (WAN) for both voice and data, companies can cut the amount of circuits at each location thus reducing another monthly cost. One of the greatest but generally overlooked advantages to VoIP is Computer Telephony Integration (CTI) into the business model. This can take many forms, but think of it this way…you can integrate anything you can touch with your computers, e.g. websites and Customer Relationship Management databases (CRM).

The Protocols of VoIP

There are several different protocols used in the deployment of Voice over IP. Sometimes a single standard is used and at other times it may be necessary to use all available protocols. The four main protocols that are used for the deployment of VoIP are: H.323, Media Gateway Control Protocol (MGCP), MEGACO/H.248 and SIP. Following is a description of these four protocols. Since this paper is based on a SIP deployment I will explain the SIP protocol in more depth. I would however like to point out in a VoIP deployment one of the biggest decisions to make is which protocol(s) are used. Secondly even though these are listed as single protocols they will and most times do work in concert and in conjunction with a subset of other Internet Engineering Task Force (IETF) protocols.

H.323 is a suite of smaller protocols to facilitate voice over an IP network. One of the drawbacks of H.323 is the large overhead due to its original design to support video. Even with this drawback, H.323 has great promise to provide interoperability between vendors and is currently widely deployed.

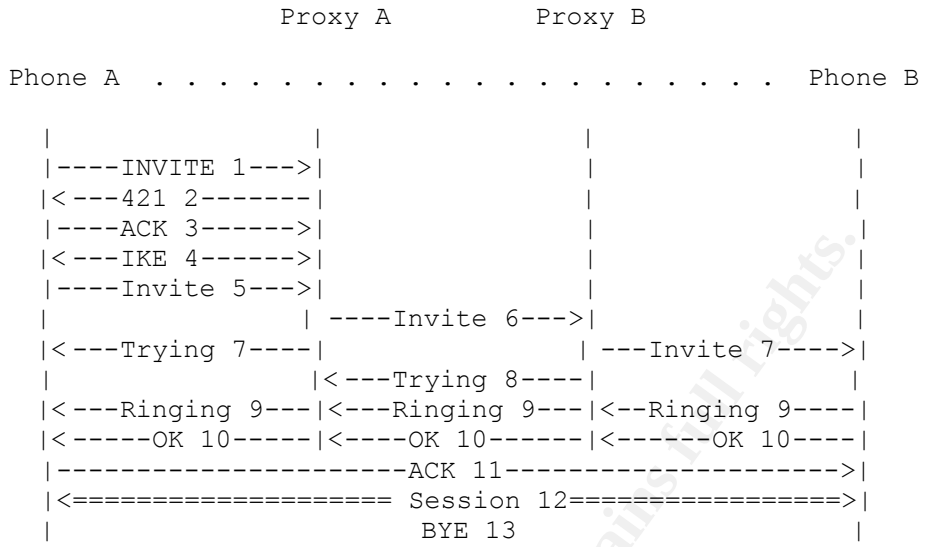
Media Gateway Control Protocol (MGCP) is the standard used for translation between a VoIP network usually using H.323 and either a Telco circuit e.g. SS7 or another gateway. MGCP relies on intelligent devices at each end (Call Agents) to handle call signaling, leaving the gateways primary function to handling of the audio signal.

MEGACO is a newer protocol that builds on the MGCP. MEGACO has a lot of promise due to inexpensive implementations and its interoperability capabilities. In MEGACO the IP phone becomes the Media Gateway (MG) that connects to the media gateway controller (MGC). This can allow for the design to scale very quickly to thousands of MGs.

What is SIP?

The Session Initiation Protocol (SIP) is generally seen as the next generation standard for VoIP. In addition to VoIP, SIP is used for videoconferencing and instant messaging. Even though SIP was designed for use with multimedia, the designers crafted this protocol in a way to be very much like other internet protocols, e.g. Hyper Text Transport Protocol (HTTP). SIP uses other traditional Internet standards like Domain Name Services (DNS) to locate identities and SIP Uniform Resources Identifiers (URIs) as an addressing scheme, i.e. caller@domain.com. This was done so SIP could take advantage of the architecture found in other popular Internet applications. By SIP working in this manner it enables User Agents (UA) to discover one another through the use of Proxy servers that UAs registers to. Once the UAs have agreed to communicate they can then carry out that type of agreed communication, e.g. voice, streaming media and videoconferencing. As a protocol, SIP only defines how sessions are to be set up and torn down. Think of SIP as the gofer asking, "Do you want to talk?" For the UAs to proceed with further interactive transmissions they must utilize other IETF protocols to define other aspects of the VoIP and/or multimedia sessions. This protocol could be the Session Description Protocol (SDP) to determine what type of media exchange will take place. Please see http://www.ietf.org/rfc/rfc2327.txt?number=2327 for more information on SDP. Then once the type of session is agreed, a protocol such as Real Time Protocol (RTP) is often used for the real time data transfer and Quality of Services (QoS). Please see http://www.ietf.org/rfc/rfc1889.txt?number=1889 for more information on RTP. As you can see SIP itself really just sets up the call, yet by SIP not putting requirements on the network, SIP can transmit any IP based network. This however can lead to many security concerns. One of the challenges of a secure SIP deployment is the fact SIP can, and most times will, transverse many devices that must all agree on a level of security if a security level is to be used, or the session will be considered failed. Also by transmitting through different points the SIP packets can not be fully encrypted for the need of devices (Proxy servers) having to add information to the header fields. Fortunately SIP does offer some inherent security in several ways which will look at in another section of this paper. For additional information on SIP please see http://www.ietf.org/rfc/rfc3261.txt?number=3261

How a SIP network call works



1. Phone A sends an Invite to its Proxy Server A
2. Proxy A sends a list of security options back to Phone A
3. Phone A acknowledges and picks the highest security that is mutual between the two.
4. Phone A and Proxy A agree on a security protocol, e.g. IPSEC-IKE or TLS, and now begin again with the transmission in a secure mode.
5. Phone A resends Invite which is encrypted
6. Proxy A does not have control of Phone B so forwards Invite to Proxy B
7. Proxy A sends a trying message to Phone A at the same time Proxy B is sending an invite to Phone B which would repeat steps 1-4 between itself and Phone B before connect is accepted.
8. Proxy B sends trying message to Proxy A
9. Phone B sends Ringing to Proxy B, Proxy B sends Ringing to Proxy A, Proxy A sends Ringing to Phone A
10. When call is answered, Phone B sends Ok to Proxy B, Proxy B sends OK to Proxy A, Proxy A sends OK to Phone A
11. An acknowledgment is sent from Phone A back to Phone B
12. RTP session is setup for duration of call
13. Call ends and bye is sent. Proxy servers log calls as ended.

How is SIP Vulnerable?

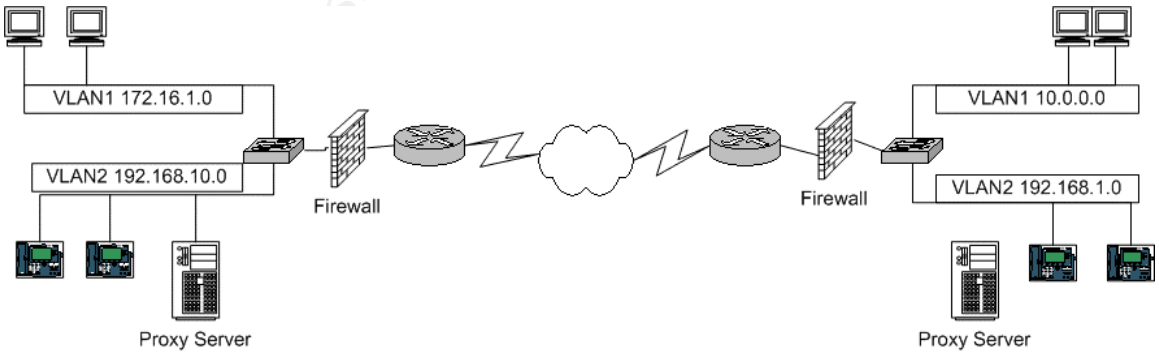
There are several threats to a SIP based network. The hardest to identify and defend against is an internal attack. Since all internal devices are to be considered trusted, detecting and stopping internal attacks can be extremely challenging. The internal attack is usually done by a UA or call participant impersonating the intended call recipient. There is also the possibility of a trusted source to eavesdrop or record the conversation for playback.

The other is an external attack. This can take the form of Denial of Service (DoS) attacks against the Proxy server, which if effective, can bring the whole call flow to a stop. External attacks can also take place when the SIP traffic is traversing a hostile environment, e.g. the Internet, or at the time a call is being passed from device to device. At any of these times the traffic is susceptible to eavesdropping, being redirected to a spoofed device and the possibility of the call being recorded for later playback. There is also the possibility of a UA impersonating another UA by changing the "from" in the header field. With a VoIP deployment there is also the chance of the server being spoofed which would cause all UA to register to the wrong Proxy thus compromising all traffic that UA may participate in.

Threats	Solutions
Eavesdropping (Call Confidentiality)	Use encryption on packets when possible
Spoofing of devices (Integrity)	Use certificates to authenticate Proxy's, address authentication for UAs
Message Integrity	Insure header information is not changed by the use of HTTP digest
Denial of Services (Availability)	Harden Server against attacks, Perimeter security

Even as we think of these issues we must also remember we still want our users to make calls with the security procedures as transparent to them as possible, yet affording the level of security need for the call.

Parts of a SIP Networks



Proxy server: The intermediate device that receives SIP request and then forwards the request on the client's behalf. In other words the Proxy's job is to forward the Invite to the next hop on the wire. Also Proxy servers can provide authentication, authorization, network access control and re-transmissions.

User Agent (Phone): These can be either a hard phone or a soft phone (a computer based program that uses the system sound card and microphone for voice transmission) located on a PC. Phones access the LAN by the IP protocol.

Switch: Used to segment traffic for better LAN performance and security by logical separating traffic.

Firewall: Used to block unwanted and possibly dangerous traffic from entering a protected LAN segment or Network.

The Proxy server

Your Proxy servers are the life of all calls and must be protected in a like manner. Depending on the vendor used will determine the Operating System (OS) that is deployed, but these general rules apply for any OS.

1. Install and configure the Proxy server out of band from the network.
   One should always install the OS on any platform in a sterile environment. This keeps root kits and other OS vulnerabilities from being exploited prior to the deployment of the system.

2. Make sure OS and any other software is patched.
   This will ensure all known security issues are resolved before system is brought online. It is always a good idea to check a bug tracking organization such as Bugtach.org for any new bugs and fixes.

3. Remove unneeded and potently dangerous services.
   Why leave a door knob on a door that will never be opened? This will help the administrator by not having to patch unused services.

4. Apply a third party benchmark such as from CIS (Center for Internet Security).
   As with anything in life a second opinion is always good. CIS is an organization that develops tools for analyzing systems to ensure they meet minimal standards for security. CIS makes these benchmarks and scoring tools for many platforms. They also receive input from vendors and the security community to make the benchmarks and to ensure that they not only meet security minimal for a lab systems, but also systems in production environments. Benchmark tools can help a busy administrator from overlooking vulnerabilities. Also benchmark tools are useful in helping your organization have a standard security objective to reach for.

5. Record a baseline on the system using a change detection tool such as Tripwire.
   This serves the purpose of giving you an objective way of telling whether your system has been modified by an intruder, and to what extent. For

such a baseline to be useful, however, it is imperative that the information be kept current and updated whenever authorized changes to the system are made.

6. Record your baseline data to secure media.
   Your baseline does you no good if it, too, has been tampered with. Have a written policy worked out with your company attorney for handling, dating, and storing data that may become evidence in a court of law. Work these policies out before you need them.

7. Apply any additional company security policies, e.g. password policy, access policies.
   These policies are important because different companies may have different security requirements. Suffice it to say, though, that strong passwords and strict enforcement of access policies are paramount in any IT security scheme.

8. Places Proxy server in a physically secure environment.
   No matter how wonderful a job is done on securing the software, if I can take your system home…game over!!

9. Place Proxy server behind a firewall with appropriate allow and deny policy for the network.
   You want the system locked away, but for it to be of service you have to allow it to interact with other systems. VoIP has special considerations in that, you do want to allow internal calls out and outside calls in. For this reason a firewall must be configured to allow traffic to pass, yet affording security against a DoS (Denial of Services) attack on the proxy and/or other unauthorized network access. A good rule is to always deny all and to setup your allow list for only the outside devices you want to allow in. For a good overview of the ports that are used and other issues with allowing SIP traffic through a firewall please see http://www.cisco.com/en/US/tech/tk652/tk701/technologies_tech_note09186a00800f2853.shtml .

10. Use access list on Proxy server to grant access for only the devices it controls.
    A Proxy server should only allow UA (user agents) or other trusted Proxy servers to attach to it. This can be done in a number of ways but the easiest and I believe the most effective is to use allow and deny files. These files should use both IP address and domains names as the identifying characteristics of the system either denied or allowed.

11. Monitor system with logging for any security violations and keep system up to date on fixes and patches.
    Diligence is important. As administrators we should never deploy a

system and not monitor it. Monitoring a system can be as easy as checking the logs daily or as complex as rehashing the software loads. Keep up on new security issues of the OS you deploy by the vendor and other mailing lists.

The Wire

Securing the wire will help in stopping the voice traffic from being recorded off the wire or from a system impersonating a trusted Proxy server or another UA. This preserves the call integrity. Also security at the wire will help in protecting against MitM attacks. As we look at securing the data path we should be focused with the actual physical access to equipment and data streams.

1. Who has access to a phone?
   One of the best ways to limit access to phones is to have a company policy that requires all users to first login to the phone each day and to logout at day's end. Also some vendors can allow the administrator to log phones out after a period of inactivity. There is some thought to having Personal Identification Numbers (PIN) for all users which would be used prior to dialing a call or at the point of picking up the hand set to receive an inbound call. This may be needed in some environs, but in most situations would not be tolerated by end users. Logging in and out can also be good in tracking WHO has made calls, to where, and at what times. Please beware in a VoIP setting, tracking of this nature can be very useful troubleshooting problems, but also could be a legal issue of privacy that should be addressed by the appropriate member of each company's security team. Also the use of logging a UA in can keep the casual passerby from accessing a phone without permission.

2. Can you be sure no new phones are brought online?
   It is very important to know the equipment you have deployed and where it is. One of the ways to combat this is network monitoring for unauthorized devices. Each Proxy server should be configured with a list of media access control numbers for devices that are allowed on net. Always keep a full detailed record of the phones that are installed with the matching Media Access Control (MAC) addresses for each UA. This is important if you need to do a scan of the network for inventory or for a general security audit. You should be able to match all phones with your documentation. This is vital in assuring no new equipment is brought online unauthorized.

3. Who may want to access to the call?
   What is your business and who is your competition? Answering this question can tell you who might want to hear your calls and what type of resources they may have. It is always best to have a defense in place for an attack that never comes, then to react after being attacked!

4. Can someone take a sniff of your traffic?
   It is very important to make it very difficult for someone to record your data stream and to then be able to analyze it at their leisure. One means of deterrence is to deploy the IP telephony devices and IP data devices in two logically disparate segments. Segmenting IP voice from the traditional IP data network greatly increases QoS, scalability, manageability, and security and attack mitigation. Segmentation of data and voice traffic via VLANS alone can not guarantee voice traffic will not be recorded or redirected. However segmentation of traffic is one of the most fundamental steps in securing a VoIP network. By using VLANs one must gain physical access to the wires to truly be effective in packet capturing. I do want to point out though that there are tools such as 'dsniff' that can be used to sniff a switched network so it can not be emphasized enough that security MUST be deployed in layers.

5. Can someone see inside your LAN?
   While security by obscurity is no security, it is still a very good idea to keep your network topology and addressing scheme from becoming publicly known. This is where a strong firewall policy and the use of Network Address Translation (NAT) come into play. By denying all with a firewall at the perimeter except for traffic you deem trusted is the best way to keep hackers from doing a network recon. One should also consider denying the following Internet Control Message Protocol (ICMP) responses, connections from private addressing on the outside interface, and denying traffic on ports that will not be used. Also never forget to monitor the logs for scans and aborted connection attempts.

SIP security Mechanisms

SIP can offer some encryption of the message body and protection of critical header fields. Even though SIP has some security built into the protocol it can not encrypt the whole packet. This is due to each hop having to read and/or alter fields in the packets. For entire message encryption one must look to a third party solution to ensure the call can not be heard in real time. The SIP security mechanisms and encryption are essential parts of the call security. Depending on the infrastructure and cost constraints the organization is willing to bear will determine the type of encryption used.

1. Selecting a security level
   First the UA will contact the Proxy with a list of the type of security it would like to use.
   Secondly the Proxy would challenge the UA to perform the security procedures.
   Thirdly the UA will choose the highest level of security both can agree on.
   Fourthly the UA contacts the Proxy with the list of security options in

response to the challenge.
Finally the Proxy verifies its own list to ensure it was not altered.

2. Authentication
   All devices should be able to use HTTP Digest authentication scheme in SIP which allows for replay protection and one-way authentication. HTTP authentication is really only useful on the first hop. After the first hop the call is relying on the Proxy or gateway to provide the net hop authentication.

3. Transport Layer Security
   Transport Layer Security (TLS) Is one method that can be chosen for security during the challenge response as described above. TLS can provide privacy for the lower layers allowing the server and client to authenticate and agree on encryption prior to any data being sent.

4. Request security for the full path
   This can be done by use of SIPS URIs. While this is similar to SIP URIs, it differs in the fact that the connection will maintain TLS till the finally hop.

5. Preserving confidentiality
   To preserve the confidentiality of a call one must encrypt the message body. SIP can do this with the use of S/MIME which can provide end-to-end confidentiality and integrity for message bodies without affecting message headers, as well as mutual authentication. It is also possible to use S/MIME to provide a form of integrity and confidentiality.

Site-to-Site Security

For greater security in a VoIP site-to-site architecture one may consider using IPSec. IPSec creates tunnels through hostile environments, e.g. the internet. This is commonly known as a virtual private network (VPN). IPSec provides many options for encryption and authentication. Connections created by IPSec can provide integrity, encryption, and authentication or at times, all three. Once two nodes have connected they must determine which algorithm they will use e.g. Data Encryption Standard (DES) for encryption and Secure Hash Algorithm (SHA) for integrity. Once the nodes have agreed on the security parameters, they then share session keys. At this point, the traffic between these nodes is effectively in a secure tunnel
IPSEC is a frame work of the following three protocols that provides encryption and authentication.

1. Encapsulating Security Payload (ESP) protocol
   ESP can provide data confidentiality, optional authentication and replay detection. ESP completely encapsulates the data being sent.

2. Authentication Header (AH) protocol
   AH can be used by itself or in conjunction with ESP. AH provides packet authentication service.

3. Internet Key Exchange (IKE) protocol.
   IKE is used to establish a shared security policy and keys for authentication services for IPSed. IPSec-IKE is great to be used when traffic is being passed between routers and firewalls, for each host must be able to identify its peer.

Final Thoughts

As VoIP evolves and becomes more widely used, it will fall to network and systems administrators to combine the voice and data traffic into a secure environment. As I hope I have highlighted, the securing of data and voice share a lot of the same challenges and characteristics. However unlike data, VoIP does have special requirements that data networks do not have and in closing I would like to leave a couple of these as food for thought.

1. Firewalls- How can we let all this dynamic traffic through without the wall crumbling?
2. VoIP end points can be any where- Can you ensure all are up to date with firmware and security patches?
3. Management of Certificates for Proxy to Proxy server- This is not that hard if they are your Proxy servers, but what good can a phone be if you can not get outside calls?
4. Let's Relay off your Proxy- SIP is in some ways similar to SMTP and as we all receive SPAM from servers that are open-relays, Proxy servers can also be open to relaying.
5. Integration of Pretty Good Privacy (PGP) for a total enterprise solution- One key does all. This is the best bet for security for all communications.

Bibliography:

Noemy Morris, Frank Childs, Charles MacMullen, Al Brisard, Judith Kelly, MCK Communications. “A Primer for Datacom Professional.” 2001. http://www.securitytechnet.com/resource/hot-topic/voip/voip4data.pdf (7 July 2003)

Noemy Morris, Frank Childs, Charles MacMullen, Al Brisard, Judith Kelly, MCK Communications. “A Primer for Telecom Professional.” 2001. http://www.securitytechnet.com/resource/hot-topic/voip/voip4voice.pdf (7 July 2003)

Greg Galitzine. “Pulling Together -- Interoperability Through Open Standards.” October 2000. http://www.tmcnet.com/articles/itmag/1000/1000spec_focus.htm#1 (7 July 2003)

CISCO Systems. “Understanding Packet Voice Protocols by CISCO Systems.” http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a008009294d.shtml (7 July 2003).

Information about H.323. http://www.openh323.org/standards.html (7 July 2003).

James Toga and Hani ElGebaly. “Demystifying Multimedia Conferencing Over the Internet Using the H.323 Set of Standards.” URL: http://www.intel.com/technology/itj/q21998/articles/art_4.htm (7 July 2003).

C. Groves, M. Pantaleo, LM Ericsson, T. Anderson
Consultant T. Taylor, Nortel Networks Editors. “Gateway Control Protocol Version 1.”June 2003. http://www.ietf.org/rfc/rfc3525.txt?number=3525 (7 July 2003)

Packetizer, Inc. “SIP Information Site.” http://www.packetizer.com/iptel/sip/ (7 July 2003)

J. Rosenbe, dynamicsoft, H. Schulzrinne, Columbia U., G. Camarillo, Ericsson, A. Johnston, WorldCom, J. Peterson, Neustar, R. Sparks, M. Handley, ICIR, E. Schooler, AT&T. “SIP: Session Initiation Protocol.” June 2002.l http://www.ietf.org/rfc/rfc3261.txt?number=3261 (7 July 2003)

A. Vemuri, Qwest Communications, J. Peterson, NeuStar.
“Session Initiation Protocol for Telephones (SIP-T): Context and Architectures.” September 2002. http://www.ietf.org/rfc/rfc3372.txt?number=3372 (7July 2003)

J. Arkko, V. Torvinen, G. Camarillo, Ericsson, A. Niemi, T. Haukka, Nokia. "Security Mechanism Agreement for the Session Initiation Protocol (SIP).) January 2003. http://www.ietf.org/rfc/rfc3329.txt?number=3329 (7 July 2003)

M. Handley, V. Jacobson, ISI/LBNL. "SDP: Session Description Protocol." April 1998. http://www.ietf.org/rfc/rfc2327.txt?number=2327 (7 July 2003)

Audio-Video Transport Working Group, H. Schulzrinne, GMD Fokus, S. Casner, Precept Software, Inc., R. Frederick, Xerox Palo Alto Research Center, V. Jacobson, Lawrence Berkeley National Laboratory. "RTP: A Transport Protocol for Real-Time Applications." January 1996. http://www.ietf.org/rfc/rfc1889.txt?number=1889 (7 July 2003)

CISCO Systems. "Guide to CISCO Systems' VOIP Infrastructure Solutions for SIP."http://www.cisco.com/application/pdf/en/us/guest/tech/tk701/c1634/ccmigration_09186a00800eadf1.pdf (7 July 2003).

CISCO Systems. "Security in a SIP based Network." http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml (7 July 2003).

Jason Halpern. "IP Telephony Security in Depth." http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a00800ad368.shtml (7 July 2003).

Johann Thalhammer . "Security in VoIP Telephony Systems." http://www.iaik.tugraz.at/teaching/11_diplomarbeiten/archive/thalhammer.pdf (7 July 2003)

Activsupport, "Physical security: first steps to a secured network." http://www.activsupport.com/network/vpn_security/physical_security.html (7 July 2003)

CISCO Systems. "VoIP Traversal of NAT and Firewall." 26 March 2003. http://www.cisco.com/en/US/tech/tk652/tk701/technologies_tech_note09186a00800f2853.shtml (7 July 2003).

Frank Thernelius. "SIP, NAT, And Firewalls." May 2000. http://www1.cs.columbia.edu/sip/drafts/Ther0005_SIP.pdf (7 July 2003)

The Center for Internet Security. " CIS Security Benchmarks and scoring tools." http://www.cisecurity.org/ (7 July 2003)

The SANS Institute. SANS 'The Twenty Most Critical Internet Security Vulnerabilities .” 29 May 2003 http://www.sans.org/top20/#W1 (7 July 2003)

J. Franks, Northwestern University, P. Hallam-Baker, Verisign, Inc., J. Hostetler, AbiSource, Inc., S. Lawrence, Agranat Systems, Inc., P. Leach, Microsoft Corporation, A. Luotonen, Netscape Communications Corporation, L. Stewart, “HTTP Authentication: Basic and Digest Access Authentication.” June 1999. http://www.ietf.org/rfc/rfc2617.txt?number=2617 (7 July 2003)

T. Dierks, Certicom, C. Allen. “The TLS Protocol Version 1.0.” January 1999. http://www.ietf.org/rfc/rfc2246.txt?number=2246 (7 July 2003