GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Security Concerns with VOIP

Eric Weiss
August 20,2001

Introduction

IP Telephony is a process that enables the transfer of voice data over a packet switched network as opposed to the traditional circuit switched networks of today's telephone companies. Companies are moving to this technology because it allows them to use their existing network infrastructure to carry both data and voice traffic. Savings come from eliminating the need to purchase new PBX equipment, and from reduced staff and maintenance costs because only one network needs to be supported. Other incentives for moving to VOIP are the possible savings from the cost of long distance per minute charges of sending voice traffic via existing carriers and the advantages of promised new features such as:

1. Internet aware telephones
2. Inter-office trunking over the corporate Intranet
3. Remote access from branch or home offices to both the voice and data networks via the Internet
4. Internet call center access

IP telephony was first introduced in the mid 1990's and has improved steadily since then in the areas of reliability and sound quality. These improvements have gone hand in hand with increased network bandwidths and improvements in compression technology, which has allowed IP Telephony to now become a viable technology.

Current voice traffic on circuit switched networks has a very high level of quality because each connection is guaranteed a certain bandwidth (64kbps) for the life of the call. When voice traffic is transmitted over an IP based network the data is compressed down to 7.9 kbps or 6.3 kbps depending on which standard is being used (G.729 or G.723.1). This saving in bandwidth comes at a price in the quality level of the call. On an IP based network, packets can travel over any number of different routes so the quality of the transmission is tied to the quality of the network. Lost packets in a VOIP network degrade the quality of the system by appearing as gaps of silence in the conversation.

As with any technology that is still in its infancy there are various standards that are being proposed as the best way to achieve industry acceptance. There are several standards in place that deal with IP Telephony implementations at the moment. This paper will briefly discuss the following three standards:

H.323 from the ITU, which was first approved in 1996 but had its beginnings in the early 1990's

Session Initiation Protocol (SIP) from the IETF, which was first approved as an RFC (2543) in 1999

© SANS Institute 2000 - 2005, Author retains full rights.

MGCP was first published by the Media Control Working Group as RFC2705 in 1999. This protocol is a combination of two other protocols: IDPC (Internet Protocol Device Control) and SGCP (Simple Gateway Control Protocol).

A basic difference between these three architectures is where intelligence is concentrated. SIP places most of the intelligence at the endpoints of the system. MGCP places the intelligence in the network components. H.323 places intelligence everywhere.

H.323 is a comprehensive protocol, which tries to address all aspects of a VOIP system. It is an umbrella system, which includes a number of other specifications such as:

H.225 - call control signaling, registration and admission
H.235 - security issues: Authentication, Integrity, Privacy and Non-Repudiation
H.245 - channel usage negotiation
H.261 - Video Codecs
G.723 and G.729 - Audio Codecs

An H.323 system is composed of four main components:

1. Terminal
   This is an end-user device, which supports two-way voice, data and/or video traffic with another terminal. An end-user terminal would be an IP telephone or a PC with VOIP software and hardware.
2. Gateway
   Gateways are responsible for communicating with other or different networks. If the connecting device on the other network is not an H.323 device, the gateway will translate between the two protocols. A gateway allows a connection from a PSTN to IP based LAN.
3. Multipoint Control Unit
   An MCU provides support for multi-conferencing between several enduser terminals.
4. Gatekeeper
   Gatekeepers provide authentication services to allow end-users to register on the VOIP network. It also manages access policies and address translation.

SIP is a less complicated protocol and hence, some would argue, more flexible. It is a challenge-response based system similar to the HTTP protocol. The main components of a SIP based systems are:

1. User Call Agent or User Agent Client
   The UAC is responsible for initiating a call by sending a URL addressed INVITE to the intended recipient.
2. Proxy server
   Proxy servers are responsible for routing and delivering messages.
3. Redirect server
   A redirect server keeps a user database, which allows it to inform proxy servers of a users location.

© SANS Institute 2000 - 2005 Author retains full rights.

MGCP systems are composed of Media Gateways, Signaling Gateways and Media Gateway Controllers. MGCP does not require end-user devices capable of complex processing, as does H.323. MGCP gateways should be able to work with both H.323, SIP and legacy telephones.

H.323 probably has more adherents than SIP or MGCP as of this writing, but that may be primarily due to its earlier release.

Security Issues

Until the present time, security issues in the data and voice worlds, while these issues are in fact very similar, have been seen to be completely separate in the minds of most users. Users have been exposed to the risks of sending data over the Internet while at the same time having the expectation that telephone conversations are strictly confidential. With the convergence of the voice and data worlds the real similarities of the security concerns will become apparent. This paper will deal briefly with four security issues that are well known in the data world.

Privacy:

On the familiar public switched telephone network people have long been aware of the possibilities for wiretapping, but these threats do not appear to be a major concern to the public because for the most part they seem to be limited to espionage or underworld crimes. For eavesdropping to occur on the switched telephone network there needs to be physical access to the telephone line and access to some type of hardware device that may or may not be very sophisticated. Only one conversation is tapped at a time. In the VOIP world the dangers are increased considerably. The equipment or software needed is much more sophisticated but not out of reach for today's expert hacker. Data sniffing tools are readily available and it will not be long before these tools are enhanced to become aware of the new VOIP protocols. Because VOIP traffic travels over a data network that is used by all of the regular users of the corporate LAN, any or all of the conversations traversing the network could theoretically be compromised by anyone with a regular connection on the network. VOIP packets could be identified and stored for re-assembly to be played back at a later time. The idea that only Internet traffic is at risk is not based on reality. Many sources have for years proclaimed that 70 to 80 percent of all hacking incidents occur from the inside. Privacy for voice traffic could be vastly enhanced by the use of encryption; however, most corporate networks do not encrypt VOIP calls. Encryption and decryption are CPU intensive and take time. If the overall latency of a VOIP call is greater than approximately 250 msec the quality of the call will be noticeably affected.

One of the attractive features provided by VOIP is the intelligence that can be located at various points in the network. Gatekeeper or call-manager type devices, which authenticate users and establish connections, can physically reside on any network server. This is really a two-edged sword. Logging information about user calls may be useful for billing or tracking purposes, but these logs can now become a target for hacking. If this

© SANS Institute 2000 - 2005 Author retains full rights.

kind of information becomes compromised it can be a serious concern to the organization. Servers containing VOIP call log information will need to be physically secured. These servers should not be running any un-needed services or daemons. In addition logins to the VOIP servers should be strictly limited.

Call Quality and Integrity:

If a data packet is lost while being transmitted over an IP network it can easily be re-transmitted. Lost VOIP packets however, will directly affect the quality of the voice transmission. Denial of service attacks have, unfortunately become all too common in today's Internet environment. As corporations convert more and more of their voice traffic to traverse their regular data networks the threat of DOS attacks will take on heightened meaning because now normal telephone service could fall prey to simple hacker tools that anyone can download off the Internet. VOIP servers will need to be placed behind "VOIP aware" firewalls. There are many security-related patches available that pertain to DOS attacks. Network administrators will need to pay particular attention to the VOIP servers on their network to make sure that the servers are always up-to-date with the latest security fixes.

Another threat that must be guarded against is the possibility of a hacker taking over a gateway device. This could be achieved by emulating VOIP signals that the gateway is expecting. This would require that the hacker has access to the gateway's network and has an in-depth understanding of the VOIP protocols. This would not be an easy endeavor, but in today's world of ingenious hacking exploits if something can occur, it probably will.

Authentication:

Just as in the data world, users of VOIP many occasionally have the need to ensure that the person on the other end of a call is really who they say they are. The H.323, SIP and MGCP standards provide mechanisms for authenticating users.

The H.235 component of H.323 specifies two types of authentication:

1. Symmetric encryption
   This method of authentication is less processor intensive and requires no previous communication between the two devices
2. Subscription based
   This method can be either symmetric or asymmetric.
   It requires the sharing of a secret key or certificate before the communication can occur. Diffie-Hellman key exchange can be used to generate the shared secret key. Symmetric encryption methods are generally very secure, however they require large amounts of CPU processing power and time.

H.235 also allows for the use of IPSEC to handle the authentication between the VOIP devices.

The SIP protocol allows for three different types of authentication, all of which are challenge-response based.

© SANS Institute 2000 - 2005 Author retains full rights.

1. Basic authentication
2. Digest Authentication
3. PGP authentication

MGCP recommends the use of IPSEC for encryption and authentication.

Non-Repudiation:

When dealing with legal requirements such as the need to prove whether someone placed or received a call the only recourse in the past had been the billing information of the Telephone Company. With VOIP there is the additional method of proof if the system has a requirement to use a public-private key encryption method such as Diffie-Hellman or PGP. In the public-private key method of encryption a call would be placed after it was first encrypted using the caller's private key and the public key of the intended recipient. The recipient or gateway could then decrypt the call using his private key and the public key of the caller. In this scenario, only the user with the specific private key could have placed the call.

Recommendations

1. Do not use shared media devices such as hubs on Corporate VOIP networks. Using a shared media device would allow a potential hacker to have access to all conversations traversing the network. This does not mean that it would be a simple task to re-assemble random packets into a recognizable transmission, but why make it easier? Network administrators will need to do periodic audits to make sure that there are no unauthorized devices snooping around on the network.

2. Vendors should be pressed to ensure that all VOIP traffic that is sent over a public IP network will be encrypted. At the present time the driving force for vendors of VOIP equipment is quality of service. Users will not accept a phone system that is not up to the standard of the plain old telephone service, which they have been comfortable with. If however, there occur several instances of eavesdropping of supposedly confidential conversations, users would immediately lose confidence in the system. End-to-end encryption, which requires the IP telephone devices to have a great deal of processing power, is not the only option. Encryption could also be done only at the link-level. Gateway devices normally are designed to handle heavier processing loads and this method should be transparent to the users. Encryption could be limited to specific fields within the VOIP packets that contain sensitive information.

3. Any VOIP server that contains potentially confidential information needs to be locked down and treated with the same security precautions as any server with a confidential database. VOIP systems have powerful management features, which can tag logged calls in many ways to help in future retrieval. With the added capabilities of storing user call data and reporting on this data easily, comes the responsibility to protect this data, as would the Telephone Company. One solution would be to place

© SANS Institute 2000 - 2005 Author retains full rights.

the VOIP servers on a separate segment protected by a VOIP aware firewall.

4. Make sure to build redundancy into the VOIP network. The ability to combine both the data and voice networks into a single network is a major economic driving force in the rapidly growing move to VOIP. This convergence does highlight some major issues though. Users have become accustomed to occasional short outages in the data network, but phone service is another story. When planning the VOIP implementation make sure to consider alternate ways to provide phone service in the event of major network problems. This is especially true for 911 services. Make sure to plan for scheduled network downtimes so that phone service can still be maintained.

5. Verify that your firewalls are VOIP aware. In some cases, an application aware proxy server that can handle dynamic ports and addressing may be needed. Be aware that by allowing VOIP packets through a firewall a potential security risk is involved. Hackers may at some point find a way to ride into a network through a firewall by manipulating an H.323 packet. When using NAT and encryption there are additional difficulties with the SIP protocol because IP addresses appear in the body of the protocol.

Bibliography:

1. Welch, Anthony K., "Security Concerns in an IP Telephony Network", IPVoice Communications, 2000, URL: http://www.ipvoice.com/IPVoiceWebSite/www/ipinvest_sound.html

2. Marjalaakso, Mika, "Security Requirements and Constraints of VoIP,Helsinki University of Technology, URL: http://www.hut.fi/~mmarjala/voip

3. "Voice over IP Technologies: Ready For The Enterprise?", URL: http://www.hermesgroup.com/whitepapers/VoIP/voip.htm

4. Black, Uyless, "Voice Over IP" , Prentice Hall PTR 1999

5. Voice over IP, URL: http://pigseye.kennesaw.edu/~dward/VoIP4.htm

6. Gifford, James, "IP Telephony: IS YOUR VOIP SECURE?", Computer Telephony, Sep. 1 ,1999, URL: http://www.computertelephony.com/article/CTM20000510S0059

7. "Security Considerations for IP Telephony Networks", Cisco Technical Solution Series: IP Telephony Solution Guide, pp. 4-87 – 4 –108

8. Kotha Sam, "Deploying H.323 Applications in Cisco Networks" URL:

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.cisco.com/warp/public/cc/pd/iosw/ioft/mmcm/tech/h323_wp.htm

9. Mednieks, Zigurd, "Is Privacy the Killer App?", URL: http://www.phonezone.com/telirati/26.shtml

10. Rosenberg, John D., and Shockey, Richard, " The Session Initiation Protocol (SIP) : A Key Component for Internet Telephony", ComputerTelephony.com/June2000 URL: http://www.ctbooks.com/article/CTM20000608S0019/1

11. Bernier, Paula, "Something Old, Something New - MGCP Provides Links to IP,PSTN" , URL: http://www.soundingboardmag.com/hotnews/8bh16161931.html

12. "MGCP", URL: http://www.webopedia.com/TERM/M/MGCP.html

© SANS Institute 2000 - 2005, Author retains full rights.

Last Updated: October 19th, 2017

Upcoming Training

SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Nashville SEC401^	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Hawaii SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event