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

Frank Echezabal
GSEC Practical Version 1.4b, option 1
March 18, 2003

Voice over Internet Protocol Security (VoIP Security)

Abstract
This paper will cover some of the issues surrounding the security concerns with the application and implementation of voice onto data networks. As well as to help the reader to understand the measures that are required in order to achieve a secure level with Voice transmissions, as it relates to convergence of these onto IP (Internet Protocol) networks. I will show different aspects of the technological, business and human effects in hopes of informing the reader to the full impact of VoIP security.

Introduction

The internet is a relatively new concept (about 10-15 years) into the way businesses and people communicate. Business has accepted the internet as a viable, reliable and economical way of communicating with partners, suppliers, customers and their own employees at distant locations. People have accepted the internet as a grand world view to products, services and information from any location all over the world. We've all accepted this along with a reasonable time of maybe 3 to 7 seconds between screen refreshes - without even a second thought.

Voice applications have been around for quite a bit longer. It's creation in the 1870's started to gain great momentum in the 1890's (1). And so since this time, the telephone, it's interfaces and protocols have been developing and improving. Along with the human acceptance of almost a zero second delay in telephone conversations.

The security on the telephone has mainly involved the securing of the physical location of phones, telephone switch systems, wire closets and telephone poles. And so interception of a call was limited if you had a pair of alligator clips. Intentional and authorized interception of a call was limited to telephone service carriers, government and business switch providers with expensive, complicated, proprietary equipment and with capable people to operate them.

Security in the internet area is very different. The internet was originally created as a forum for communications between universities and military. IP Security was not in considered at the time. As a result, the security of the internet is not bound by the ISP's (Internet Service Provider) equipment, enterprise routing equipment, wire closets and telephone poles. But, to every increasing number of internet user at home around the world or in an office just down the hall.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Even before the tragedies of September 11, 2001, the internet had been increasing with attacks, intrusions and espionage to government and business databases and servers. And so after 9/11, security analysts took a more detailed look at how the internet was being used in the goals for terrorism. After all, it was the best way for the network of terrorists around the world to communicate.

What is voice ?

Voice is a sound just like music or noise, in that when it is carried on a wire it is reduced from the original frequency range (heard naturally or with high performance equipment) to a range that can be transmitted and is then known as analog voice. Voice transmissions (telephone conversations) are a real time application. To appreciate this just think of the annoyance of a conversation with someone and when it is unknowingly interrupted. It requires a certain level of quality so that the conversation flows well and becomes an enjoyable experience. And thus cannot be measurable by technical equipment but, by arbitrary research and compilation. MOS (Mean Opinion Score) is such a test defined by the ITU recommendation p.800. Below is the criteria for the scoring (2). It should be noted that toll-quality voice must achieve a score of 4 or above. MOS scoring is a long-standing subjective method of measuring voice quality.

Score	*Listening quality*	*Listening effort required*
5	Excellent	Complete relaxation possible; no effort required
4	Good	Attention necessary; no appreciable effort required
3	Fair	Moderate effort required
2	Poor	Considerable effort required
1	Bad	No meaning understood with any feasible effort

Security on voice transmissions

Today's voice conversations without even considering the "over IP" part is under strain. For those of us who thought that our phone conversations were not to be compromised – think again. Law enforcement has been trying to pave the way for intercepting calls (3). The government, FBI and CIA have historically had the capability to wiretap calls at service providers. But, now the internet is not part of that alliance – it involves a far greater number of ISP's and enterprises, making it much more difficult to wiretap internet calls. National security is at stake, consider the efforts of Dutch Intelligence in trying to conduct wiretapping only to be leaking information to another country (4). The FBI is involved in this case but, how long will it be before the capabilities of the FBI are exhausted with the potential that the internet could bring. Private corporations are at stake, consider the conversation that occurred with the heads of HP concerning the HP/Compaq merger which was acquired by the San Jose mercury news (5) and posted it to its Public Web site. It talks about confidential conversations that were used on a proxy fight and also used against the merger. Sure it was on a voice mail, but what about conversations that are not recorded. A sniffer can record in the same

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

manner and be played back later. Lastly, consider a call that you could have with a cousin, doctor or banker discussing something that you consider sensitive. What if someone in your neighborhood found out about some personal, medical or financial situation that you just didn't want others to know. How would that affect you ?

Security with VoIP transmissions

To begin, there are IP security issues that affect most all networking products; clients, switches, routers, servers and IP devices. VoIP and convergence exposes previously secure products to new attacks dealing with service, privacy and authentication. The internet, intranet and LAN networks each have their own types of attacks. Vulnerabilities and attacks happen daily and are constantly being announced through several publications. Software developers (i.e. Microsoft) are taking extra steps to ensure product integrity.

The internet is so vast and diverse that the need and desire to make things easy have driven it to be what it is today. Computers used to be for code crunching people with the technical expertise to dive deep into the inner workings of systems. Products like standards based modular chassis, components, higher generation programming languages and point-and-click interfaces have made great advancements. One of the negative points to this standardization is that it allowed any virus or attack to affect a wider user-base (i.e. Melissa virus on Microsoft operating systems). Plainly speaking, VoIP is voice transmitted over IP, and IP packets can be intercepted with easy to use tools that are freely available on the Internet. This makes the profile of the attacker much broader, so that people can learn and use these sometimes sophisticated software tools very easily.

Sniffers were originally designed for troubleshooting and capturing information on data networks. VoIP audio packets are vulnerable to sniffers and can be recorded and replayed or even listened to in near real time. Now, unauthorized access can happen in the privacy of someone's office in the building or perhaps across the continent. Vomit (Voice over Misconfigured Internet Telephone, (6)) is one such tool that is easy to use with it's standard GUI based interface, has the ability to detect the packets of a conversation, decode G.711 calls, organize them in a sequential manner, record the session and convert to a standard ".WAV" file format.

It was thought of for some time that having an ethernet switch would make each port coupled with VLAN configurations would make a user more secure. However (7), there are tools available to not let ethernet switches be a problem.

Ethernet switches direct traffic based on destination address to specific switch ports. If each switch port has one host, that host will see traffic destined for Itself, unlearned destination MAC address locations, multicast and broadcast. Certain

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

switches are vulnerable to forwarding table attacks using attack tools like “Angst”, “Macof” and “Dsniff”. Switches can be flooded with random MAC addresses, thereby overflowing their own forwarding table and causing them to transmit frames out all port on a VLAN. Certain switches will forward duplicate frames out to the same MAC address located off of different ports. The MAC address of many Unix machines can be quickly changes using a one line command,

“#ifconfig eht0 hw ether ??:??:??:??:??:??”

Arp spoofing, man-in-the-middle and arp poisoning can be done with tools such as arpredirect (part of the Dsniff suite).

Relaxed switch management can attribute to misconfigured trunk ports which provide easy entry to inter-switch network traffic, port mirroring by unauthorized personnel or for unauthorized purposes to mirror VoIP conversations to sniffed ports. Vulnerabilities also lie with wireless 802.11 protocols which operate in a similar environment to shared Ethernet (CSMA/CA). Even with static WEP, all users can “hear” each others network traffic.

Encryption

Encryption is the process of mixing up the transmission so that the recipient can use a key (or process of un-mixing) to acquire the original message. During transmission, without the key, it would just seem like a bunch of useless text.

Encryption happens between the users input to the application (OSI application layer) and the cable (OSI physical layer) by which the input is exiting the input device. The actual location is the OSI session layer. This is right above where the Real Time Protocol takes shape. For the purposes of this paper, the output of the codec (g.711 or g.729) is encrypted using an algorithm and is placed in a payload area without affecting routing or prioritization. This algorithm could be very long to make the possibilities of breaking the encryption code. And sometimes is shorter due to constraints in the processors involved, costs or importance of the data.

At the moment one of the strongest encryption lengths that provides maximum protection is 128bit encryption. Why not use 128bit encryption for everything ? The process of encrypting and decrypting uses a lot of computing process resources. If 128bit encryption is going to provide a call which is very secure and unrecognizable – then what’s the sense. Keep in mind that the telephone endpoints are not pentuim 4 machines and that this is a real time application. So efficiency is important. A creative way of providing a difficult pattern to break may be to use different algorithms for different tasks. One way could be to use an alternating 56bit pattern during a call when it wont affect the quality of the call and maybe use a difficult 128bit pattern for the initiation of the call – before the

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

people begin to talk. This encryption process add very little latency (3ms) end to end.

128bit encryption has a very good reputation and requires significant computing resources. And even though the 56bit encryption has been broken by using several computers working in parallel after about 22 hours. It doesn't discount it as an unusable algorithm. It is possible to break – anything can be broken. 56bit is not trivial to break. The idea here is that this is not government level encryption and to add a layer of complexity and difficulty without allowing simple or clear text to traverse the network.

Solutions for VoIP security

Currently, VoIP packets are sent in clear text out of the originating device. A secure solution is needed to provide privacy for VoIP - for sensitive information. It needs to be simple and transparent for users. Difficult solutions usually have a way of being worked around to avoid inconvenience and delays. It should provide:

- Wiretap protection, for audio IP streams
- Encrypted session key generation
- Secure distribution of keys
- Extensibility to other, future encryption algorithms (AES)
- Work with unsecured devices
- Work between endpoint – not just the WAN

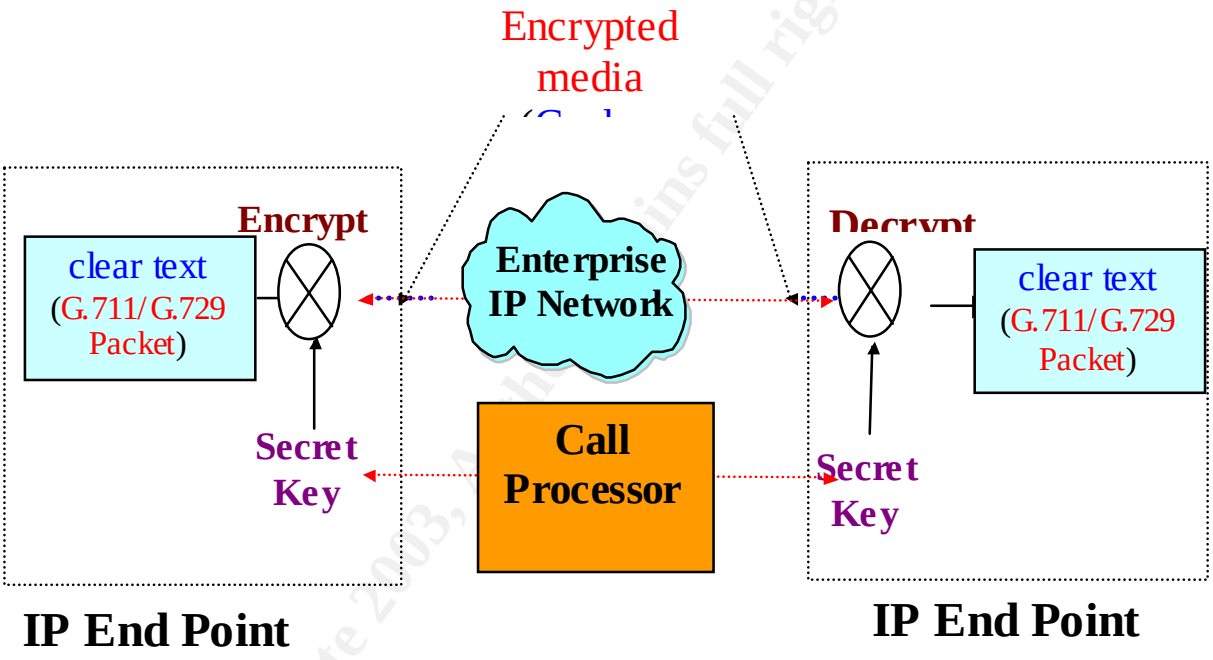
Cisco, Nortel Networks and Avaya Communications are the most recognized vendor names in enterprise convergence equipment with VoIP capabilities. Given the vulnerabilities listed and the technology available. Most vendors are offering a VPN (Virtual Private Network) either with dedicated point to point, Frame Relay or encrypted tunneling to resolve the security issues. These remedies are sufficient for the Wide Area Network. But what about at the local and remote enterprise sites, beyond the firewall and routers. These solutions don't protect the LAN – this is where most unauthorized activity occurs.

Cisco understands the vulnerabilities with Vomit (8), Here's an excerpt from the article "Following the guidelines in this document does not guarantee a secure environment, *or that you will prevent all penetrations.* It is the intention of the author to provide you with enough information such that you will make an informed choice as to the risks and benefits that the technology holds. Only after you have weighed the risks and benefits should you deploy any technology. "

Nortel networks also promotes the use of VPN's to create an encrypted tunnel with this document (9), "Securing Voice over IP (VoIP) across the Internet How Nortel Networks Contivity portfolio".

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Avaya Communications is the only one that satisfies all the features listed above and will encrypt the VoIP conversation from end to end. Avaya's "Media Encryption" will initiate a session key for each call. And will not be susceptible to the vulnerabilities of Vomit or other call sniffing tools. From the diagram below notice how the encryption occurs within the endpoint devices. An encryption key is transmitted to each endpoint. The endpoint then use this key to encrypt before sending any packets and decrypt before receiving any packets. Clear text is never transmitted into the network. All transmissions within the network are encrypted.



Sure, it might not be fully standards compliant. However, it is the best option of being most reasonably secure and publicly available in the market today.

Future solutions for VoIP security

Security is an increasing concern to technology. Previous standards like H.323 have not been very effective. It is often viewed as a security risk given that H.323 uses many different and dynamic TCP/UDP ports. SIP (session Initiation Protocol) has shown the most promise. Showing compliance to all the requirements in the previous section. SIP (10) is a signaling protocol for various VoIP and instant messaging applications. It creates and manages a session between endpoints. These sessions are guided by the endpoints and my have different addressable names with different media (simultaneously). This would involve several protocols to carry a variety of real time applications. SIP sounds like a great flexible protocol for creating, modifying and terminating sessions. At

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

this time even before SIP is used for general purposes, it is blemished with several vulnerabilities (11).

Any protocol or provision that would work to secure real time VoIP would need to be at the RTP layer 4 or above. No standards exist today but, IETF drafts are in initial stages of a Secure Real Time Protocol (SRTP) (12). Conceptually this is a good idea because it works with what already exists.

Impact of VoIP security on business

Business is business. Before any installation considers a real time application like Voice over IP, they must do an in depth analysis of their network as it relates to the quality of the data transmissions. This process is not necessary for the pure data network because the applications have the ability to overcome issues like the second screen arriving first and to have to resend the seventh page because it was lost. We accept these delays as we sit and look at our computer screens saying "Hmmm the system is a little slow". A voice conversation could not withstand these complications – we'd rather say "Hey, listen …I'll call you another time". This alone could involve a separate discussion. Of the main issues would be to see if the network could support the following within tolerable limits:

Delay

Delay is the amount of time that a data network packet takes from the sender's application to reach the receiver's destination application. Round trip delay is obviously the time that a data network packet would take from the sender's application to the receivers application and then back to the originators application.

Jitter

Jitter is the variation in delay of the packets as experienced at the receiving end. If packets experience varying delays such as 75 – 125 msec, as they arrive, the data transfer is said to have jitter. This is when you might hear a choppy voice from the remote side.

Packet Loss

Loss of packets in the network could happen due to congestion or heavily loaded networks. Packets are dropped due to buffer overload in routers, switches and other networking equipment. The human ear will not detect a few packets being lost during transmission – as long as the conversation appears to be continuous and without significant interruptions.

Prioritization

Prioritization covers several areas, generally it's the configurable mechanisms that can be put in place to distinguish and react accordingly to different types of packets. These can involve CoS (Class of Service) to tag or label packets so that subsequent steps can recognize and process the packet properly. Switched

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ethernet networks should have IEEE 802.1p/q compliant equipment to also recognize and process the packets properly. Other measures could include switch port prioritization.

As you can see, if a data network is working fine from a business point of view – why fix it. These limits could pose an issue of having to spend for much more money on equipment, management or resources. Security then takes a backseat to these issues. Unless the business decision is from the top and is recognized and evaluated from a return on investment and forward looking point of view, companies would rather stay where they are. Issues like the slow inception of VoIP to the market place coupled with equipment that might not be QOS or VoIP aware are also reasons for slow market share. Small enterprises that can venture out have been more predominant that large enterprises but, large enterprises are evaluating them and about 40% are in testing stages now. IP telephony has a lot of potential. Sales grew 21% year over year to $171 million in the second quarter of 2002. So you can see how this could be a driver for market share in this sector with any equipment vendor.

Now consider if a business overcomes these obstacles and decides to continue to build out their network to provide VoIP capabilities. One would then have to encompass a whole new philosophy about security. After all it's not like a piece of equipment that you install, configure and walk away from. Security is a process that requires mindset of ongoing maintenance, upgrades, policies, analysis and training. Trained and experienced security professionals are highly paid. Confidentiality issues (HIPPA…), trade information, security policies, risk analysis, privacy and authentication take on a new meaning.

Conclusion

There are many issues surrounding the implementation of secure Voice over Internet Protocol. People have been using the telephone for many more years than the computers. Generations of people have benefited from the sense of making secure phone calls from the privacy of their home or office. People have come to expect a high level of reliability and security from the telephone and telephone systems – which grows every time a data system is out of service or needs to be booted. Just think about it. How many times does the telephone system require a restart, as opposed to the data system or a computer. Sure, these systems have been around to stand the test of time. But, more importantly the issue is the perception that has taken generations to form. People that judge, procure and use these devices will definitely have an impact on the future and the outlook for secure VoIP. Businesses will slowly take steps towards VoIP in order to benefit from the reduced management and cost savings that a converged system will bring – and maybe security will be a consideration. With time, the protocols will be perfected, bandwidth will be abundant and economical, and security will be just another transparent function that will be built in and forgotten.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

References

(1) Casson, Herbert N. . The History of the Telephone, December 1999, http://etext.lib.virginia.edu/toc/modeng/public/CasTele.html

(2) Vinnie Servis, Measuring voice quality over VoIP networks, December 2001, http://www.tolly.com/News/NewsDesk/20011219VSVoIP.asp

(3) Carolyn Duffy, Bid to allow Net wiretaps draws fire, October 1999, http://www.cnn.com/TECH/computing/9910/27/wiretap.protest.idg/

(4) Paul Wouters and Patrick Smits, Dutch tapping room not kosher, December 2002, http://www.fnl.nl/ct-nl/archief2003/ct2003-01-02/aftappen.htm

(5). Michelle Quinn and Tracy Seipel, Fiorina voice mail reveals late scramble, April 2002, http://www.siliconvalley.com/mld/siliconvalley/3031960.htm

(6) Niels Provos, vomit - voice over misconfigured internet telephones, http://vomit.xtdnet.nl/

(7) Tom King, Packet Sniffing In a Switched Environment, August 4, 2002, http://www.sans.org/rr/netdevices/packet.php

(8) Jason Halpern, SAFE: IP Telephony Security in Depth, June 2002, http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safip_wp.htm

(9) Nortel Networks, Securing Voice over IP (VoIP) across the Internet How Nortel Networks Contivity portfolio, Feb 2003, http://www80.nortelnetworks.com/query.html?charset=utf-8&ht=0&qt=%22securing+voice+over+ip+%28voip%29++across%22&qs=&qc=&pw=100%25&ws=0&la=en&qm=0&st=1&lk=1&rf=0&rq=0&si=0&col=nnprodpg&col=hotlinks&col=hpocs&col=nncorp&col=nnemp&col=nnglob&col=nnprd&col=nnpress&col=nnprod&col=nnsol

(10) Network working group, RFC 3261 Session Initiation Protocol, June 2002, http://www.ietf.org/rfc/rfc3261.txt

(11). CERT, Multiple implementations of the SIP vulnerabilities, VU#528719, http://www.kb.cert.org/vuls/id/528719

(12). IETF, The Secure Real-time Transport Protocol, June 2002, http://www.ietf.org/internet-drafts/draft-ietf-avt-srtp-05.txt

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Last Updated: April 28th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS