A Brief Overview of VoIP Security

By John McCarron

Voice of Internet Protocol is the next generation telecommunications method. It allows to phone calls to be route over a data network thus saving money and offering increased features and productivity. All these benefits come at a price, vulnerability. It is easier to attack and exploit a voice and data network. VoIP will need extra security measures beyond the standard security that is typically implement for a computer network. Many issues need to be addressed such as type of attacks, security, quality of service and VoIP protocols.

There are many VoIP protocols in the market. Some are proprietary while others are open standards. The two most popular open protocols are H.323 and SIP. They were designed by two different organizations and operate slightly differently. They both have problems with the use of random ports problems with NAT translations and firewalls.

H.323 is an International Telecommunication Union standard for audio and video communication across a packet network (National Institute of Standards and Technology 2005). There are four types of devices under H.324: terminals, Gateways, Gatekeepers and Multi-Point Conference Units. The terminals are phones and computers. Gateway provides an exit to other networks. The Gatekeeper handles addressing and call routing while the MCU provided conference call support. H.323 uses other protocols to perform other vital tasks. UDP packets using the Real-Time Transport Protocol transport all data. H.225 handles registration, admissions & status, and call signaling. H.235 also handles all security and has four different schemes call Annexes. “H.323 is a complicated protocol” (Tucker 2004).

Session Initiation Protocol (SIP) is a signaling protocol for Internet conferencing, telephony, presence, events notification, and instant messaging (Schulzrinne 2006). The Internet Engineering Task Force developed this VoIP protocol. SIP is an application layer protocol that uses TCP and UDP. The protocol is designed to work with servers and endpoints such as phones. There three types of servers. The location server maintains a database of the location of all endpoints. The proxy server passes the calls between networks while the registrar server authenticates all traffic. SIP can use HTTP, SMTP, IPsec and S/MIME, Secure/Multipurpose Internet Mail Extension, for security instead of creating new methods. This makes it a lot simpler than H.323 (Tucker 2004).

There are many different methods that VoIP can be attacked or exploited. Some attacks try to steal information while others attempt to shut down your network. The attacks include eavesdropping, spoofing, denial of service, call redirection, and replay attacks.

Eavesdropping is the unauthorized interception of voice packets and the decoding of the conversations. It is relatively easy and simple. There are many free network analyzer, sniffers and packet capture tools that can convert VoIP traffic to wave files (Roberts 2005). This allows you to save the files and play them back on a computer. Vomit, Voice over Misconfigured Internet Telephones, is an example of such a tool (Provos 2004). Typically eavesdropping is restricted to the subnet the phone is attached to and the path it takes to the destination. The National Security Agency is able to eavesdrop on all international calls coming into or out of the United States. This is done by placing Narus STA 6400 data mining equipment at all major telecommunication

centers such as AT&T. Narus' machines are able process 622 megabits worth of voice traffic a second (Bewert 2006).

Replay attacks are used to gain more information about the source network. A packet is captured and retransmitted into the network to generate more traffic to be captured and analyzed. This allows for more information about the network. These attacks are often a prelude to other attacks such as man-in-the-middle and spoofing (Roberts 2005).

Packet spoofing uses a false source address on the IP packets. The network data such as a VoIP call will appear from a different often trust source than where it originated. This is also known as masquerading. Spoofing can change caller ID number, hide the origin of attacks, and pretend to be a trusted host. Several services available allow you to spoof your phone number. Such providers are Telespoof, PI Phone, Spooftel and Covert call. Asterisk, a free open source program, can also spoof numbers but is designed as a call manager (Roberts 2005). A serious risk with spoofing is identity theft.

Call redirection occurs when a call is intercepted and rerouted through a different path before reaching the destination. This could lead to eavesdropping, call fraud, and illegal use of your networks. If your network is compromised, the call could be redirected through the network to hide the source or to charged the phone calls to your company (Roberts 2005). In addition, your call could be illegally redirected to a service that charges you with out your knowledge. "Communication Fraud Control Association estimates annual world-wide telecommunication fraud losses to be in the range of 35-40 billion U.S. Dollars" (NIST 2005).

Denial of Service is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic (DoS 2004). VoIP is more susceptible to DOS than a typical computer network. Not only does it suffer from the standard DoS attacks of flooding the network with traffic to the point it crashes but it also has its our specific vulnerabilities. VoIP specific DoS attacks use setup and "cancellation of pending call set up signals … including sending a CANCEL, GOODBYE or PORT UNREACHABLE message" (Roberts 2005). This causes the phones not being able to complete calls or hang up. With DoS there is a chance that both you data network goes down along side of your phone services provided through VoIP.

VoIP has many security vulnerabilities that need to be protected. Encryption, Virtual LANs and Firewalls are a necessity on all networks that deploy VoIP. Also Network Address Translation should be avoided. These are a few important features that need to be addressed.

Encryption helps protect your privacy and authenticates the message. Transport Layer Security and IPsec are the two main encryption methods. IP security is used to encrypt call setup and control messages. TLS is an alternative to IPsec and is based off the SSL protocol. It is used is used to provided an secure call setup. Many different algorithms can be used such as DES, 3DES, AES, RC4, and RC5 (Roberts 2005). The simpler encryption results in better performance (N.I.S.T 2005). It is an effective measure against eavesdropping and protects sensitive information.

Firewalls are a standard security feature on networks. They protect the network from attacks by inspecting each packet that travels to and from the network. Firewalls have trouble filtering VoIP traffic due to dynamic port assignments through out the call.

Both SIP and H.323 requires stateful firewall to track the traffic and associate the port numbers. "Stateful firewalls remember previous traffic and can investigate the application data in a packet" (N.I.S.T 2005).

All Voice over IP traffic should be routed on separate VLANs than the data networks. This while make it harder to have both your data network and VoIP network compromised. Viruses will have a harder time infecting both sides of your network. It also makes it more difficult to sniff, intercept, or eavesdrop on traffic when it is divided up into separate VLANs (Tucker 2004).

Another typical feature on a network is Network address translation. NAT provides a method of changing private IP address in to public ones. It also allows for port translation. It is a method to conserve IP addresses and add another layer of security. Along with these benefits come problems with VoIP. NAT complicates VoIP call set up and traffic. Dynamic assigns random port numbers to traffic when there is a pause and the translation times out.(N.I.S.T 2005) This makes it hard for VoIP equipment to track and maintain calls. IPv6 will reduce the need for NAT with the introduction of the 128-bit network address. "The best solution is not to use NAT if at all possible" (Tucker 2004).

While attacks affect quality of service, some security features can have an impact. Features such as NAT, firewalls and encryptions affect the VoIP QoS. The three main issues are Latency, Jitter, and packet loss.

Latency is the amount of time it takes to transit a packet to its destination. Throughout the call process, many things can cause delays. Encrypting and encoding typically takes up to 30 ms while sending the packet might take up to 100 ms (N.I.S.T

2005). A latency of 150ms is comparable to the standard PSTN phone system (Tucker 2004).

Jitter is non-uniformed packet delay (N.I.S.T 2005). This caused when packets have different latencies and arrive at the destination at different times. The packet then will need to be reassembled in the correct order. Voice of IP relays on UDP packets for transportation which are connectionless and do not provide sequencing at the protocol level. The VoIP applications will have to reorder the packets. Routers, Firewalls that support QoS along with buffers can help alleviate the problem of jitter.

Packet loss can have a crippling effect on VoIP. High latency, excessive jitter, or low bandwidth all can cause packet loss. It is the most noticeable issues. One to three percent packet loss is the maximum threshold before there is serious loss in service quality. While the loss of more than five percent of the packets drops the quality of service below that of analog telephones.

Security is a necessary part of any computer network. VoIP has many vulnerabilities to attacks such as Spoofing, Eavesdropping, and Denial of Service. VoIP needs to be protected beyond the standard measures. VLANs and Firewalls need to be configured to support VoIP traffic. Encryption should be used while NAT is avoided. All security measures needs to balance protect with quality of service of the network.

References

Bewert. (2005). *All About NSA's and AT&T's Big Brother Machine, the Narus 6400.* Retrieved April 12, 2006, from http://www.dailykos.com/storyonly/2006/4/8/14724/28476

National Institute of Standards and Technology. (2005). *Security Consideratins for Voice over IP Systems* (NIST Special Publication No. 800-58). Gaithersburg, MD: U.S Department of Commerce. *

Provos, N. (2004).VOMIT - *Voice Over Misconfigured Internet Telephones*. Retrieved April 12. 2006, from http://vomit.xtdnet.nl/

Roberts, C. (2005). Voice over IP security. *Center for critical Infrastructure Protection.**

Schulzrinne, H. (2006). *Session Initiation Protocol (SIP).* Retrieved April 12, 2006. from http://www.cs.columbia.edu/sip/

Sicker, D. C., & Lookabuagh, T. (2004). Voip security: Not an Afterthought. *QUEUE*, , 56-64. *

Tucker, G. S. (2004). Voice over Internet Protocol (IP) and Security. *Sans Institute* *

What is a DoS attack?(2004). Retrieved April 12, 2006, from http://www.webopedia.com/TERM/D/DoS_attack.html