VoIP – Time to Make the Call?

By Steve Sullivan

Abstract

Is it time to make the call and join the growing numbers of companies that are embracing Voice over IP technologies? Even though VoIP is a relatively new technology, it is maturing to the point where companies of almost any size can take advantage of the cost savings and added features. Network Administrators have a tough job providing their users with the security and reliability that they have grown used over the years. But, with proper equipment and network design, there is no reason companies of all sizes can't make the move to the third generation of the phone system.

This paper will examine some security concerns and defense approaches by looking at the threats to VoIP and how to deal with them from design, quality of service and management perspectives.

VoIP – Time to Make the Call?

By Steve Sullivan

Companies are beginning to embrace VoIP technology for a variety of reasons. But has VoIP evolved to the point that companies can expect the same reliability and security that they have grown accustomed to with the public switched telephone network (PSTN) that has been the standard for many years. This paper will look at the current threats to VoIP and examine if the current security efforts are enough.

VoIP is a method for sending voice traffic as data over traditional IP-based networks. The biggest reason companies are interested in this technology is the cost savings. Traditionally companies have purchased one set of hardware and software for their voice communications and a completely different set of hardware and software for data communications. By consolidating these systems into one, not only are companies saving money on hardware costs, but many times they are seeing additional savings from reduced workloads for setup, support and system changes. As an added bonus, VoIP also offers many new features that are impossible for traditional phone systems. But just adding VoIP traffic onto your existing data network is not the way to have a successful implementation of VoIP. A VoIP implementation must be carefully planned out and the network must be designed to specifically handle VoIP traffic. This paper will examine how far VoIP has come and if it is secure enough to provide the same level of

performance businesses have come to rely on from the public switched telephone network for over twenty-five years.

The Technology

VoIP is the third generation of the phone system. The original phone systems were all analog. They converted the voice signal into analog electrical waves and they were converted back on the other end. In the 1950s digital networks replaced the analog networks. In a digital network, the voice signals are converted to 1s and 0s and sent digitally over the phone network and converted back on the other end. This was done with a series of repeaters and since all the signals were either a 1 or a 0 then they could be created on the far end nearly identically to how they were transmitted. This eliminated the major problem of the analog phone systems where noise is amplified when the analog signal gets amplified as it gets weak over distances. With analog networks, the longer the distance was, the lower the quality. This loss in quality was practically eliminated with digital networks.

The digital networks used for phone system are circuit-switched networks. A dedicated circuit is built when the call is placed; all of the traffic for the call travels over the circuit, then the circuit is torn down once the call is over. In the last twenty years packet-based networks have become the norm for data communications. In a packet based network the information to be transmitted is broken into small packets that each have their own routing information. Each of these packets is then able to find its own path to the

destination where they are re-assembled into their original form. The internet is an example of a very large packet-based network. VoIP is a technology that takes voice calls and transmits them via public and private packet-based networks rather than traditional circuit-based networks.

VoIP calls consist of two main components, the bearer portion that carries the actual voice communication and the signaling portion that contains the information for creating and ending the call. Because voice calls are very sensitive to delays, VoIP employs two basic techniques to help eliminate those delays. First VoIP calls are carried in Realtime Protocol (RTP) packets which were designed for the transmission of time sensitive data. RTP packets are carried by standard User Datagram Packets (UDP) but RTP adds packet sequence information, so the packets can be played in the right order, and time stamping to help endpoints manage Jitter which is discussed later.

The second technique is the use of standard voice encoding algorithms called codecs which compress the data and manage the call quality. By compressing the data, less information has to be transmitted which helps maintain QOS.

The Threats

Most of the threats to VoIP are the same as those you would have in two separate networks. The threats against data on the data network remain the same but now their reach is much greater because they can now affect voice communications in addition to

data communications. A Denial of Service (DOS) attack against a router or a call-processing server could take out phone communications. Impersonation attacks and Man in the Middle attacks, where a device is fooled into sending its packets to the wrong device where they are captured and dissected, could allow access to the network and critical data.

Then there are threats that are specific to VoIP. VoIP protocols run over IP. A few years ago, VoIP manufacturers all had different standards and protocols which were closely guarded company secrets. But as the technology has evolved, the need for increased interoperability has made the Session Initiation Protocol (SIP) & H.323 the most widely-used. SIP was developed by the Internet Engineering Task Force (IETF) and is open source code which means that just about anyone can get a copy of the source code making it much easier for hackers to find ways to exploit it. Even though the source code is open, if properly implemented, SIP can provide secure voice communications using IPSec (IP Security). H.323 was developed by the International Telecommunications Union (ITU) and is a host of protocols that not only cover VoIP, but also cover video and other services. H.323 also has security functions that can be implemented to provide a higher level of security.

There are threats to gateways and other call processing machines. If a hacker was able to gain access to a media gateway that connects the network to the Public Switched Telephone Network (PSTN) then they could potentially make free phone calls, reroute calls or disrupt service to other users.

There are also Operating System (OS) vulnerabilities on machines that run critical components to a VoIP network such as call-processing software for PBXs. Most of these applications run on either a Microsoft Windows-based or Linux-based box. Hackers are constantly attacking Microsoft products and finding ways to crash or exploit the Windows operating systems. Linux is open source code and has vulnerabilities too. Vulnerabilities that exploit the OS could take down all voice communications by taking down a call processing server. Viruses and Worms could affect voice communications by attacking these same call-processing machines. Trojan Horses and Spy Ware can find their way onto IP networks and steal confidential information, network bandwidth and affect the Quality of Service (QOS) of voice communications.

Finally there are the same types of threats that affect traditional voice systems and in many instances it is actually easier to exploit VoIP. Software like Vomit (Voice Over Mis-configured Internet Telephones) already exists and is readily available to eavesdrop on VoIP calls. Service-theft attacks could still be carried out where someone is able to make long distance calls for free. A phone could be configured to forward phone calls to a long-distance number or someone could call in and get an innocent employee to forward the call.

Adding VoIP to your data network does not really present any new threats. What it does is place more reliance on the data network and security measures that are often over-looked, will now need to more closely examined.

Start with Design

To successfully secure your VoIP implementation, a multi-layered defense scheme will be needed. A simple secure the perimeter plan with not be able to handle the sophisticated type of attacks that hackers are using today. Hackers have two things that make them successful: time and money. They have plenty of time to figure out weaknesses and exploit those weaknesses. These days they have plenty of money as well. Many of the security breaches you read about are tied to organized crime. I read an article recently about a security breach at a major retailer and before the break-in was even discovered, over a million dollars in merchandise was charged on the stolen credit card numbers. This is not the work of a single individual holed up in a computer room somewhere proving that no system is secure. That was the profile of the hackers from years ago. Today they are organized units that have a plan to not only break into a system, but also what to do once the break-in is complete.

Design security throughout the network. Don't just build a strong perimeter defense trying to keep everyone out. Multiple layers with security throughout the network will make it harder for a hacker to traverse the network if they were able to somehow get past the perimeter defenses. On the perimeter layer you will find things like routers and firewalls. It is important to make sure these devices are designed to handle the VoIP packets specifically so they are able to address the unique security needs of VoIP and most importantly be able to prioritize traffic to maintain QOS for VoIP. Using VoIP

aware networking equipment will allow you to take advantage of the network layer security in SIP and H.323 the two main signaling protocols for VoIP.

At the host layer security revolves around the individual devices. Making sure they are hardened by eliminating any default user names and passwords and locking out the ability for users to change the configuration. These endpoints can potentially be exploited to gain access to the network itself. You would also include host-based virus protection and individual firewalls to the host layer defenses. On the critical components such as Media Gateway Controllers (MGC), Media Gateways (MG) and PBX systems you should employ intrusion detection systems (IDS) to ensure undesired access to the network hasn't occurred. You can also employ an IDS on most Cisco routers which will help build security throughout the network since these routers are typically used to build and control traffic on the network.

Finally at the application layer, you can make sure that applications do not have the ability to make changes to the system like starting or stopping a service. Encryption of data for transmission also takes place at the application layer. Encryption can greatly reduce the risk of eavesdropping, but it must be implemented carefully to avoid QOS issues. Anytime there is encryption/decryption there is a performance hit and it must be managed to ensure QOS does not suffer. Finally, Host-based Intrusion Protection Systems (HIPS) can monitor and protect the key hosts.

Quality of Service

VoIP is a relatively new technology so you don't hear much about systems being exploited. In fact, it is probably easier to tap into a standard phone line and eavesdrop on a call than it would be to capture VoIP packets and recreate a phone conversation out of them. Let's face it, they both require physical access to the building or network. For standard phone line, a handset that is available at most electronic stores is all that is needed to tap into a copper phone line. To eavesdrop on a VoIP call, once physical access to the building has been gained, the hacker would then have to connect to the network somehow and start sniffing packets to try and find a voice conversation between two endpoints amongst all the many packets that are traveling down the wire. If he does happen to decode the Ethernet packets and find a stream and somehow look deep into the protocol stack and determine it is a voice communication, he would still have to decode the IP and transport layers to get to the voice packets. Those voice packets would be encoded with one of many formats and may be encrypted on top of that. That is a lot of work for a hacker to go through to listen to a phone call.

Since eavesdropping isn't that easy, one of the bigger threats against VoIP would be an attack against QOS. These types of attacks could disrupt voice communications and generally cause havoc to the network. Let's face it, if you are downloading a file and the network slows down for a couple of seconds then it won't really affect you. Even if it completely stopped for 5 seconds and then continued your download, you may never even notice and it certainly would not adversely affect you. However, any delay over about 150 milliseconds can create problems for voice communications. With VoIP the

voice communication is broken into many small packets that get routed to their destination. These packets need to arrive at the destination in order and in a timely fashion. Since the receiving phone is basically "playing" what is receives, if the packet isn't there when it is time to be played, then the VoIP phone has no choice but to play silence. This variation in the arrival times of voice packets is called Jitter. Systems deal with Jitter by using a buffer to hold the packets before they are played so they can be played in a continuous stream. This gives the phone a chance to receive the packets before they are played. This works fine as long as the Jitter is less than the buffer allocated to it. If the Jitter exceeds the buffer then the phone must play silence.

There are many aspects of ensuring QOS but most of it revolves around two main areas: ensuring the network has enough bandwidth to handle the amount of data it is expected to carry and prioritizing packets so that time sensitive packets are given a higher priority than data packets. Creating VLANS to isolate VoIP traffic away from the rest of the network will help with both of these areas. There are also other tools to help with the bandwidth management like RSVP (Reservation Protocol). When using RSVP, endpoints signal the network reserving capacity for their use prior to making the VoIP call. By separating the VoIP traffic, you are also minimizing the chance that someone will be able to "sniff" the packets and eavesdrop on the phone conversation. Using VLANs with Access Control Lists (ACL) can prevent a denial of service attack from traversing across the network and affecting all users.

Another key consideration is the equipment used to build the network. Many of the routers and networking hardware components in use were installed before VoIP became so popular. This means the older networking equipment may not be specially designed to handle VoIP traffic. In a network that has both data and voice traffic, often referred to as a converged network, special priority has to be given to voice traffic. If this doesn't happen, then QOS for voice calls will surely suffer since everything will be handled on a first come, first served basis. This will force voice traffic to wait for data traffic which will have a negative affect on voice QOS. Associated with this prioritization is the use of three Type of Service (TOS) bits that are part of the IP packet. These three bits can be used to designate up to eight different priority levels that routers and media gateways can use to prioritize packets.

Manage and Monitor the Network

For years voice systems have been rated by what they call the five 9's. The five 9's is 99.999% uptime which is less than 6 minutes of downtime per year. It doesn't matter if it is a traditional phone system or a VoIP phone system, care must be taken to ensure that the system is performing as expected and not being abused. In a VoIP environment it is the network administrator who has to ensure the reliability that users have come to expect from the Baby Bells. Having 99.999% uptime does not and should not be the target reliability for most businesses. This is particularly true in a VoIP environment where many of the key pieces run over top of Windows Operating Systems. These Operating Systems need to be updated and a year's worth of updates will certainly take more than 6

minutes to install with the required re-boots. But the network does need to be available when users need it so there are many steps that can be taken to ensure things are operating properly. The more hours a system has to serve its users each day, the more reliant on voice communications a business is, and the price of everything will be the main factors when determining how many of these steps need to be taken.

- Call logs – Call logs list calls made which can be analyzed for abnormalities.
- Process monitoring – Having a separate system that ensures the primary system is operating correctly. This could be as simple as having the primary system send a message to the monitoring system at a regular interval.
- No Upgrade Downtime – This usually involves some type of mirrored server setup where one server can be updated then put in place and the 2nd server gets updated.
- Automatic Failover – A backup system that takes over in case of certain types of failures
- Geographical Redundancy - Stand by systems in different locations.

The network will also have to be closely monitored to handle any problems and detect any abuses. Call tracing to troubleshoot "noisy" connections is more involved on a VoIP network. The packets can take multiple routes and there is so much data that complex software programs are needed to analyze the data. That is on a well designed network where routers, Media Gateway Controllers (MGC), and Media Gateways (MG) all work

together. Bandwidth will also need to be closely monitored to ensure that any potential cost savings aren't wasted by over buying bandwidth. Conversely, QOS will take a hit if too little bandwidth is purchased.

Summary

VoIP is a relatively new technology that can offer companies expanded functionality at a lower cost. But the newness is wearing off quickly as more and more companies are embracing the technology. New products and equipment are making the jump more and more attractive.

The bottom line is that if you have security policies in place that protect your data network, then much of the work preparing for a VoIP implementation is done. A layered defense strategy with security built throughout the network will protect your VoIP and data networks. Expanding data security policies to cover VoIP equipment and doing the same things with VoIP endpoints to protect them as you do with data endpoints will help VoIP provide the same reliable phone service users have grown used to.

References

Practical VoIP Security, First Edition, March 2006 by Thomas Porter and Jan Kanclirz, Jr. ISBN: 1-597-4906-01.

Vagle, Jeffery. 2005. How secure is VoIP? Retrieved from the World Wide Web on April 4, 2007 at: http://www.itmanagersjournal.com/articles/8331?tid=81

Sherburne, Phil and Fitzgerald, Cary. 2004 You don't know Jack about VoIP retrieved from the World Wide Web on March 28, 2007 at: http://www.acmqueue.com/modules.php?name=Content&pa=showpage&pid=203

Mcbride, G. & Bumgarner, J.2005. Implementing Secure VoIP in the Enterprise. A Lucent Technologies White Paper retrieved on November 20, 2006 from the World Wide Web at: http://www.lucent.com/livelink/090094038009a064_White_paper.pdf

Taylor, Stephen. 2003 Is VoIP secure? You make the call. Retrieved from the World Wide Web on March 27, 2007 at: http://infosecuritymag.techtarget.com/2003/voipsecure.shtml

Vijayan, Jaikumar. October 2002. VOIP: Don't overlook security. ComputerWorld.com. Retrieved from the World Wide Web November 20, 2006 at: http://www.computerworld.com/securitytopics/security/story/0,10801,74840,00.html

Sotillo, Samuel. 2006. Zfone: A New Approach for Securing VoIP Communication. Retrieved on November 23, 2006 from the World Wide Web at: http://www.infosecwriters.com/text_resources/pdf/Zfone_SSotillo.pdf

Collier, Mark D.2004 Firewall Requirements for Securing VoIP. Retrieved from the World Wide Web on March 28, 2007 at: www.securelogix.com

McCarron, John A brief overview of VoIP security retrieved from the World Wide Web at: http://www.infosecwriters.com/text_resources/pdf/Voip_JMccarron.pdf