Securing a Converged Network

By Steven Sullivan

Abstract

Network security has traditionally been viewed in business as more of a cost than a benefit. But the latest trends are towards converged networks where voice, video and data are sent over the same network infrastructure. This change presents new challenges for network professionals and network security is playing a bigger role than ever.

Traditional voice only networks are circuit-switched and virtually secure. Sure they can be listened in on, but physical access is required which makes it much more difficult. VoIP and other new technologies are taking traditional circuit-switched communications and sending them over packet-based networks creating a whole new area of concern for network security.

In a converged network every voice port, telephone, IP phone or IP based device is a potential open door. This paper will examine what is required to secure a converged network to provide the same type of worry –free communications that circuit-switched networks provided for years.

Securing a Converged Network

By Steven Sullivan

Network security has traditionally been viewed in business as more of a cost than a benefit. But the latest trends are toward converged networks where voice, video and data are sent over the same network infrastructure. This change presents new challenges for network professionals and network security is playing a bigger role than ever. How can a converged network be secured to provide the same type of worry-free communications that traditional phones lines have provided for years?

The Difference in Technology

For the better part of the past twenty-five years, businesses have put two completely separate systems in place to meet their needs. They would put in some type of Phone/PBX system for voice communications and a data network for their information technology needs. Because of the design of voice systems, security concerns were minimal. When placing a standard phone call, a dedicated circuit is set up between the two endpoints of the phone call. All of the traffic is sent over that dedicated circuit. Since the components that create the dedicated circuit are basically all within the phone companies control, to eavesdrop on a call you actually need physical access to the circuit. The phone companies already have mechanisms in place that control the capabilities of the endpoints and control access. This prevents most abuse and makes disruption of service a rarity that is easily tracked. Call logging, access logging and numerous other techniques make long distance abuse and toll fraud easy to detect. The bottom line is the phone companies do most of the work providing security for voice communications and, through proper training, network specialists at a particular business had very little to worry about.

With the growing popularity of the internet, businesses are getting more connected than ever. Increased connectivity with suppliers, online business transactions, emails, message sharing, telecommuting and e-commerce are all areas that successful businesses are getting involved in. The evolution of IP networking has now moved into voice communications and businesses are beginning to embrace the technology to save money and add features. Voice over IP (VoIP) breaks a phone call into thousands of IP packets that are sent over public and private IP networks and then re-assembled at the other end thus eliminating the need for a separate voice network and creating a single “converged” network. Now information technology professionals will be able to wire a building for one system and use it for voice, video, and data. Additionally, if carefully implemented, VoIP can save a company on every phone call it places by eliminating the time and distance charges imposed by telecom providers.

Threats and Vulnerabilities

It's not hard to find a story about a recent security breach. They are in the news or written up on security websites on a daily basis. If you do a search for "security breach" on Google you will get over six millions hits. But before a company can provide the level of security needed for uninterrupted voice communications in a converged environment, it must first understand the threats and vulnerabilities that are out there.

Most of the threats in a converged network 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. 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.

VoIP protocols run over IP. A few years ago, VoIP manufacturers all had different standards and protocols which were closely guarded 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 source making it much easier for hackers to exploit. 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 also Operating System (OS) vulnerabilities on machines that operate critical applications 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. It could be easy to eavesdrop on voice calls in an unsecured converged network. Software to do it like Vomit (Voice Over Mis-configured Internet Telephones) already exists and is readily available. Service-theft attacks could still be carried out. 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.

A converged 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 Policies

Putting VoIP onto a network that already has security issues could be disastrous. The migration to a converged network is the perfect time to re-evaluate security policies and procedures that are already in place and make changes where needed. Strong security practices are more important than the most high-tech security software on the market. A policy must be developed that covers the known vulnerabilities and threats and maintains acceptable risks. This policy needs to be the foundation for the network design. A good security policy for a converged network will cover the following areas:

> Disaster Recovery - In a converged network, there is more reliance on the network than ever which means disaster recovery plans need to be re-evaluated to ensure acceptable downtimes are still valid.
>
> Passwords – There needs to be a strict policy concerning passwords and how often they are changed. A strong password that is changed on a frequent basis is one of the best ways to prevent unwanted intrusions. But, you have to educate the employees because no policy will work if someone visiting the building is able to get a password from a post-it note hanging on a monitor.
>
> Secured Access - The passwords on the actual networking equipment need to be even more secure. If administrative control is lost on a router or firewall, then the network will be compromised. When connecting to or performing administration on network components, secure shell (SSH) or transport security (TSL) should be used.
>
> Virus Protection - Viruses are a very real risk and the virus patterns need to be constantly updated. This is another area where education can play a major role in preventing attacks. Many viruses and malicious websites rely on the gullibility of the computer operator so a well educated user is one of your best defenses.
>
> Operating System Updates - OS vulnerabilities are discovered on a regular basis and the best defense is to keep current with the critical updates. Policies need to ensure that all machines get updated and the key components get updated as quickly as possible.

The key is to plan for the long term so that security can be added and implemented as the network grows. The security policy will need to constantly evaluate the threats and vulnerabilities to determine the risks. It will need to plan for those risks as well as a host of unknown risks. It will need to be constantly updated to account for new threats. Most importantly, it must be followed because many of the best plans fail because they stay on the paper they were written on.

Layers of Protection

A single layer of defense isn't enough these days. Spending all your effort building and maintaining a strong perimeter and relying on that perimeter to protect everything behind it just doesn't work with the sophisticated attacks that hackers are now able to carry out. For a security model to be successful, it must have several layers of security that address a wide variety of threats. Most models define four or five layers of security. The object is to create more work for the hackers to get at your data. If you can create enough work that it's not worth the effort of a hacker, then you can significantly lower your risk.

Perimeter Layer

The perimeter layer is always the first line of defense. It is where your network ends and the rest of the world begins. Firewalls are the key component in the perimeter layer. They provide traffic control by examining the packets and only allowing the proper ones into the interior network. They also perform Network Address Translation (NAT) which keeps the addresses of key components and the internal structure of the network secure.

In a converged network, it is important to use firewalls and perimeter devices that are SIP or H.323 aware. These devices are specifically designed to handle the unique needs of VoIP traffic and maintain security. Devices that are not specifically designed to handle VoIP traffic may be able to move the packets successfully but will not provide the additional security needed to avoid VoIP threats.

A critical component for VoIP security is an application–layer gateway (ALG) which handles VoIP traffic between the unsecured outside network and the secured inside network. ALGs are integrated into firewalls and can look into VoIP packets to ensure that the call setup messages are valid.

There is an area in the perimeter layer called the DMZ (demilitarized zone) that contains components that need to interact with the outside world but are too open to be completely behind the firewall. This includes mail gateways, network virus scanners, web servers and certain DNS servers. By putting these devices in the DMZ, firewalls will still control traffic and can provide some protection but they are still open enough to interface with the unsecured outside world.

Virtual Private Networks (VPN) connections terminate in the perimeter layer at a router, firewall or server in the DMZ. A VPN connection is a type of encrypted, secure connection that should be used for all remote and wireless laptop connections. By using high-level encryption, it creates a connection that is virtually as secure as a private connection. By enforcing all remote users and connections to use them, you can greatly reduce your exposure to a number of risks.

Network Layer

Most companies, especially small and medium-sized companies, are fairly open about their network behind the perimeter. This makes it easy to traverse across the network if a hacker is able to gain access. The network layer security covers all the components for the local area and wide area networks. Depending on the size of the company, it could be very complex and include everything from desktop PCs, servers, phones, fax machines, printers to remote office connections and point-to-point wan connections.

In a converged network, one of the first steps you can take to improve network layer security is to create VLANs and separate the voice traffic from the data traffic. VLANS are implemented with switches and routers and they logically separate the traffic into separate networks. This will help prevent attacks on the data network from affecting voice communications and improve Quality of Service (QOS) which is critical for VoIP. Firewalls, gateways and routers need to be able to recognize and examine SIP and H.323 packets to give them priority. By using devices designed to handle SIP and H.323, security can be enforced by requiring each request to be authenticated and authorized which reduces the chance of proxy server impersonations and DOS attacks. SIP and H.323 packets can also be encrypted and authorized using IPSec and H.235 respectively to add even more security.

Another Network Layer security function is to control access to the network by ensuring proper standards for all endpoints. This will help prevent attacks from inside the network. Control wireless access by using MAC address access lists and not broadcasting Service Set Identifiers (SSIDs). Desktop and notebooks PCs must be authenticated by computer and user. As networks get larger, using security software that ensure endpoints have proper software versions, patches, virus protection definitions and no prohibited software before allowing access greatly increases network security.

Finally Intrusion Detection Software (IDS) should be run and monitored. This can be a daunting task since IDS produces large amounts of data and many false positives. It needs to be constantly tuned and monitored which can be labor-intensive. Obviously not every business will need to take every step here. The larger and more complex the network is, then the more attention that needs to be paid to its network security.

Host Layer

The host layer covers security of the individual servers, desktops, switches, routers and other devices on the network. Every device has configurable options that can open it up to attack. All devices should be configured such that only the needed services are running and only valid user accounts exist. There should be controls on access to any configurable settings or functions like installing software. There are many host layer software packages that run on desktops and servers allowing administrators centralized management of what hosts can access and perform. This is highly desirable in a converged network since it will help prevent attacks that could take down the foundation of the network and interrupt voice and video communications.

IP phones have several host layer security features that can be employed. Most IP phones have some type of digital certificate that identifies it on the network and can be used to control access and limit unknown devices from gaining access. Also password protecting or limiting access to any configurable settings and disabling un-needed PC ports further protect PC phones.

On desktops and servers, individual firewalls and virus-protection provide an additional layer of security over the network layer protection. Disabling un-needed services, protocols and ports and restricting access to configurable settings further protect the individual hosts.

Finally on the most important hosts, host-based intrusion detections systems can be employed to provide the highest levels of security. Host-based IDSs work like network layer IDSs except they are fine-tuned to run on a specific host. When properly administered, they provide a very high level of security. Administrators of mission critical hosts may also want to employ host-based vulnerability assessment tools which scan the host for vulnerabilities. Host layer security measures can be labor intensive but when properly applied, dramatically increase a converged network's security.

Application/Data Layer

Application and data security begins with controlling access. Making sure that only the users that should have access to applications and data are the ones that do have access. Many applications are not written with security in mind, especially ones that are being used on the internet or developed in-house. One of the strongest things that can be done is using an application shield or application firewall. These are tuned for a specific application and make sure that security polices are enforced. For example on an email server, an application shield could prevent an incoming email message from starting or stopping a service or running a program on the email server.

On applications where data is entered by users, particularly on web-servers, validating the data as it is entered can reduce risks by helping to maintain data integrity and avoiding exploits. As an example, accepting only numbers on zip code and phone number fields prevent corrupt data from being captured. Also command-like words like run or execute can be filtered and prevented from being entered to help avoid exploits.

In addition to policies that control access to critical data, a policy covering encryption should also be in place. Encrypting data when it is stored and transmitted can be a last resort in case the network is compromised. This is particularly true in a converged network where encryption of VoIP calls can greatly reduce the risk of eavesdropping. Encryption should be used cautiously because encrypting and decrypting data can reduce an application's performance and place additional overhead on server CPUs.

Conclusion

VoIP is here to stay. Technologies have evolved enough that it is attractive for companies of all sizes to migrate to a converged network for reduced costs and increased productivity. But doing so puts more strain on the data networks which may already be under-protected. The good news it with proper planning, maintenance, and administration the risks can be managed.

No single layer defense will stop todays sophisticated or even the not-so-sophisticated hacker. Multiple layers of protection must be used and the more critical the data, the more layers are needed. No company can afford to overlook security as more and more reliance is placed on the core network structure and connectivity with the outside world is increasing. As bigger companies put up stronger defenses, the smaller companies with less sophisticated defenses will become easier targets. Many of the steps referenced here do not require big budgets, but rather strong policies that are well thought out and strictly enforced and can be implemented by companies of all sizes.

References

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

Pogar, Joel A. Data Security in a Converged Network. 2003. A Seimans White Paper. Retrieved on November 23, 2006 from the World Wide Web at: http://enterprise.usa.siemens.com/company/downloads/white/security/mainColumnParagraphs/01/document/SIcurity_news_release_W1348.pdf

Securing Business Communications Applications in Converged Networks – Best Practices. July 2005. An Avaya White Paper Retrieved November 20, 2006 from the World Wide Web at: http://www.avaya.com/master-usa/en-us/resource/assets/whitepapers/mis2753.pdf

Securing Your Network for IP Telephony. 2005. A Cisco Systems White Paper Retrieved November 20, 2006 from the World Wide Web at: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns391/c654/cdccont_0900aecd801e6159.pdf

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

Enterprise VoIP Security Best Practices. 2006. A Juniper Networks White Paper Retrieved from the World Wide Web November 20, 2006 at: http://www.juniper.net/solutions/literature/white_papers/200179.pdf

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

Meany, Chris. November 2002. Securing Converged Networks. Retrieved from the World Wide Web on November 20, 2006 at: http://www.tmcnet.com/it/1102/1102sie.htm

Messmer, Ellen. April 2006. Telecommuting security concerns grow. NetworkWorld.com. Retrieved from the World Wide Web on November 22, 2006 at: http://www.networkworld.com/news/2006/042406-telecommuter-security.html?page=1

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

Hickey, Andrew R. November, 2006. VoIP security safeguards -- they may be there already ComputerWeekly.com. Retrieved from the World Wide Web on November 22, 2006 at: http://www.computerweekly.com/Articles/2006/11/09/219844/VoIP+security+safeguards+--+they+may+be+there+already.htm

Tillwick, H. & Olivier M. June 2004. A Layered Security Architecture: Design Issues. Information and Computer Security Architectures (ICSA) Research Group. Department of Computer Science, University of Pretoria, South Africa. Retrieved from the World Wide Web on November 22, 2006 at: http://icsa.cs.up.ac.za/tiki-download_file.php?fileId=9