VoIP Security Challenges:

25 Ways to Secure your VoIP Network

from Versign Security, Dec 01, 2006

VoIP technology has the tech geeks buzzing. It has been touted as:

- the killer of telecoms
- a solution for the third world's communication gap
- revolutionizing factor in international business

But despite all the buzz, and the predictions that everyone will be it using it by 2009, why does it seem that every time you make a phone call with Skype the quality sucks…or that your Vonage calls constantly get dropped…or worse, that teenage hackers are stealing your personal information and bringing down the whole network?

A VoIP network is susceptible to the usual attacks that plague all data networks:

…viruses, spam, phishing, hacking attempts, intrusions, mismanaged identities, Denial of Service (DoS) attacks, lost and stolen data, voice injections, data sniffing, hijacked calls, toll fraud, eavesdropping, and on and on and on.

The only difference is, with other technologies people take basic steps to protect themselves. With VoIP, nobody is doing so. As a result, all we hear about in the mainstream media is how vulnerable and unreliable VoIP is. And let's face it…until people start taking the steps to safeguard their networks, this technology isn't going to go places.

So for those you geeks who want to see the technology get broadly adopted, (and maybe fulfill some of the lofty aspirations mentioned above) start by first protecting your own VoIP network, and then helping to protect those of your

friends and neighbors. Pretty soon, we can dump the “vulnerable” label and start gaining some non-techie fans.

So without further adieu, here are 25 ways to help you get started.

1. **Restrict all VoIP data to one Virtual Local Area Network (VLAN):** Cisco recommends separate VLANs for voice and data; this helps prioritize voice over data and also keeps traffic on the voice network hidden from those connected to the data network. VLANs are also useful in protecting against toll fraud, DoS attacks, and eavesdroppers listening in and taking over conversations. A VLAN is an effective closed circle of computers that does not allow any other computer access to its facilities; with the lack of a PC to launch attacks, your VoIP network is quite safe. Even in the case of an attack, the disruption caused is a minimum.
2. **Monitor and track traffic patterns on your VoIP network:** Monitoring tools and intrusion detection systems can help identify attempts to break into your VoIP network. Scrutinizing your VoIP logs can bring to light irregularities such as international calls made at odd hours or to countries your organization has no ties with (toll fraud), multiple log-on attempts like in a brute-force attempt to crack a password, or a surge in voice traffic during off-peak hours (voice spam).
3. **Lock down your VoIP servers:** Servers should be secured physically against both internal and external intruders who can intercept data using sniffing techniques, either within the LAN or at the ISP when data travels over the Internet. Since VoIP phones have fixed IP and MAC addresses, it’s easier for attackers to try to worm their way in. Which is why Gary Miliefsky, founder and CTO of NetClarity, recommends locking down IP and MAC addresses that allow access to the administrative interfaces of VoIP systems, and putting up another firewall in front of the SIP gateway. This will restrict incoming access to IT administrators and prevent hackers from getting in.

4. **Use multiple layers of encryption:** It's not enough to just encrypt the data packets that are sent out, you have to encrypt call signaling too. Encrypting voice packets prevents voice injections where interceptors can insert their own words into the conversation, giving it a whole new meaning. Steve Mank, CEO of Qovia, cites two common methods of encryption - the Secure Real Time Protocol (SRTP) which encrypts communication between endpoints, and Transport Level Security (TLS) which encrypts the whole call process. Encryption of voice traffic should be supported by providing strong protection at gateways, networks and hosts.

5. **Build redundancy into VoIP networks:** Be prepared for the day DoS attacks or viruses threaten to bring your network crashing down – create a network that tolerates failures by setting up multiple nodes, gateways, servers, power sources, and call routers, and hooking up with more than one provider. Don't stop with just putting the infrastructure in place; run frequent trials to ensure that they are working well and are ready to take over when the primary network fails.

6. **Put your equipment behind firewalls:** Create separate firewalls so that traffic crossing VLAN boundaries is restricted only to applicable protocols. This will prevent the spread of viruses and Trojans to servers in case clients are infected. The maintenance of security policies also becomes simpler when each firewall is considered separately. Choose networking and security vendors who support both the Session Initiation Protocol (SIP) and the International Telecommunication Union's H.323 protocol. Firewall configurations have to be created so that the appropriate ports open and close when necessary.

7. **Update patches regularly:** The security of a VoIP network depends on both the underlying operating system and the applications that run on it. Maintaining patch currency for both the OS and VoIP applications is imperative in protecting against threats from malware. A study from

Forrester Research urges companies to make sure they provide "added security measures for IP telephony, without assuming that vendors will respond to each and every risk that appears with patches for installed products."

8. **Keep your network away from the Internet:** The University of Houston is a pioneer in this security approach – the institution has put its call manager and network out of direct access from the Internet; its IP PBXs are in a domain separate from its other servers and access is restricted.
9. **Minimize the use of softphones:** VoIP softphones are prone to hacker attacks, even when they are behind corporate firewalls, because they are used with an ordinary PC, VoIP software, and a pair of headphones. Also, softphones do not separate voice and data, and are vulnerable to the viruses and worms that normally infect a PC.
10. **Perform security audits on a regular basis:** Running checks on administrative and user sessions and service activities can help bring irregularities to light. Phishing attempts can be thwarted, spam can be filtered out so it doesn't clog the network, and intruder attacks can be stopped.
11. **Evaluate physical security:** Make sure that only devices and users who are authenticated and pre-approved gain access to your network by limiting access to the Ethernet ports. Administrators are often fooled into accepting softphone devices that are not permitted on the network because hackers can easily imitate IP and MAC addresses by plugging into an RJ44 port.
12. **Use vendors who provide digital security certificates:** When IP phone vendors provide digital certificates to authenticate devices, users can ensure that the conversation is secure and is not being broadcast to other devices. The phones load digitally signed images to ensure that the software loaded is authentic. Verisign has been a pioneer in providing

authentication certificates for wireless IP phones, in an effort to prevent "tapping" (illegal eavesdropping) and "spoofing" (illegal tampering) of conversations.

13. **Secure your gateways:** Configure gateways so that only those who are allowed access can make and receive VoIP calls. Lists with authenticated and approved users can ensure that others are prevented from using the lines to make free calls. Protect gateways and the LANs behind them with a combination of an SPI firewall, application layer gateways (ALG), network address translation (NAT) tools, and SIP support for VoIP soft clients.

14. **Manage servers separately:** VoIP call servers are often the targets for attackers because they are the heart of any VoIP network. Critical weaknesses inherent in the server include its operating system, and the services and applications it supports. To minimize the chance that hackers get at your VoIP servers, manage traffic to them separately from VoIP signaling and call traffic.

15. **Sort SIP traffic:** Looking through your SIP traffic and checking for abnormal packets and traffic patterns that are different from the usual will help in cutting short sessions that are not genuine. Anomalies in the syntax and semantics of SIP and events that are irregular and out-of-sequence indicate that attacks are taking or likely to take place.

16. **Examine call setup requests at the application layer:** VoIP calls are susceptible to hijacking by outsiders who gain access to the network. Set up appropriate security policies so that only those call setup requests that conform to them are accepted.

17. **Isolate voice traffic:** For external communications, rely on a Virtual Private Network (VPN). Separate your voice and data traffic to prevent unwanted ears from listening in on your conversation. According to Kevin Flynn, senior manager of unified communications for Cisco, the biggest

problem for organizations is “bad stuff from the data network getting on to the voice network.” He recommends blocking PC port access to the voice VLAN.

18. **Use proxy servers:** Protect your network even beyond firewalls by using proxy servers to process data that comes in and goes out. Authentication and integrity are ensured when signaling messages travel between user agents and SIP proxies by integrating SSL tunnels with SIP proxies.

19. **Run only applications that are necessary to provide and maintain VoIP services:** The very fact that VoIP applications use data that is encrypted could lead to them being used to launch DoS attacks. Attackers can hide behind the cloak of encryption to avoid their activities from being monitored.

20. **Configure applications against misuse:** Prevent your network from being used to perpetrate toll fraud, phishing scams, and illegal calls by preparing a list of permitted caller destinations.

21. **Add endpoint security layers:** Use network admission techniques and IEEE 802.1X port-based network access controls to keep out devices that are not authorized on your LAN or WLAN. Network Access Control (NAC) applications are available from Cisco - Network Admission Control (NAC), Microsoft - Network Access Protection (NAP), and TCG - Trusted Network Connect (TNC).

22. **Restrict access according to certain criteria:** VoIP network administrators can set up strict admission criteria to prevent access to devices that are potentially unsafe – when they are found to be infected with viruses or worms, when they do not have the latest patches, or when they do not have the right firewalls. These devices can be redirected to a disparate network that makes them compliant and then lets them onto the main network.

23. **Avoid remote management:** If possible, it is better to stay away from remote management and audits; but when necessary, use Secure Shell (SSH) or IPsec (IP Security) for the purpose. Access your IP PBX from a system that's physically secure.
24. **Use IPsec tunneling rather than IPsec transport:** Tunneling and transport are two different encryption modes that support secure exchange of packets at the IP layer. The use of IPsec transport encrypts only the data while hiding the source and destination IP addresses. This prevents administrators from finding out who initiated the call when they analyze traffic.
25. **Secure your VoIP platform:** VoIP platforms that support the clients are built on operating systems that should be "hardened" to protect the integrity of the networks that run on it and keep out cyber attacks. Disable services that are not absolutely necessary and use host-based methods to detect intrusion.

Securing a VoIP network is an uphill task, especially when you consider the lack of standards and procedures in place. How secure a network is depends on the right choice of both hardware and software. Without a doubt, VoIP communications can be made more secure and reliable than regular PSTN interactions if the appropriate security measures are in place. So get out there and make the changes to your own networks…