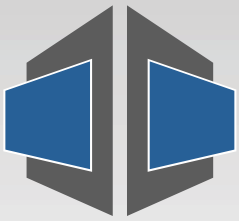
VoIP Vulnerabilities

What You Need to Consider When Assessing Business Phone Systems



COMPARE BUSINESS PRODUCTS

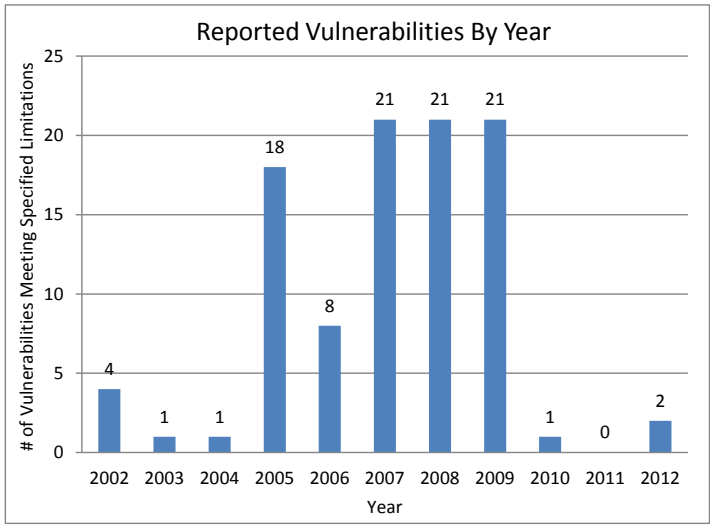
Introduction

VoIP is one of the most important developments in telecommunications after Alexander Graham Bell said in one of his first telephone calls - “Watson, come here! I want to see you!”

Improvements in the telecom space tended to be incremental for a long time and disruptive changes occurred infrequently. Major improvements occurred with switched circuits, automated exchanges and now with the maturing of VoIP technology. VoIP is based on new technologies that have opened up new opportunities and given new capabilities to voice based communication systems. Low cost and greater flexibility are other important benefits.

Many administrators assume that since VoIP uses data networks, the same security that holds good for data networks would suffice for VoIP systems as well and that they can simply plug in VoIP components into LAN ports and get on with their work. Unfortunately this is not true; VoIP has its own characteristics that make it different from plain old data.

Because VoIP relies on software to perform its magic, software vulnerabilities play a role in making the system less secure. The following graph, courtesy of the National Vulnerability Database[1], indicates a number of reported vulnerabilities over a 10 year period.



As you can see, 2005 – 2009 was a particularly turbulent period. This coincided with the early growth phase of the technology when a number of small and large vendors introduced VoIP products.

Many of these products had vulnerabilities that were reported by researchers and security companies. It is a sign of the rapid maturing of this market that the numbers of vulnerabilities have reduced rapidly.

This paper looks at some of the major reasons why VoIP security needs differ from other data security needs and how this influences the construction of VoIP networks. We will also discuss the major VoIP security threats and how these can be circumvented. Some best practices will also form part of the paper.

[1] http://web.nvd.nist.gov/ view/vuln/statistics

Quality of Service and the Difference between Traditional Data and VoIP

Since VoIP is a real time application, performance demands from enterprise VoIP systems are very stringent. Quality of service (QoS) is a key parameter. If you have used any of the free voice calling applications on the Internet and have experienced delays, echo and jitter, you know what we are talking about.

Implementation of various security measures will have an impact on impact on QoS unless the system is built from the ground up with QoS and security in mind. Security equipment could cause delays in transmission at firewalls, encryption / decryption may cause excessive latency and there is a naturally low tolerance for packet loss. Intrusion detection systems impose additional penalty due to inspection of data packets.

While any of these delays would have been acceptable in a data system, in VoIP applications their overheads are frowned upon. Therefore, administrators must understand that VoIP security needs and solutions are necessarily very different from those of other data systems.

Firewall and NAT Issues

No security solution exists without firewalls. These form the first line of defense for any network. However, most firewalls introduce complexity into VoIP infrastructure and interfere with dynamic port management and call setting up.

Network Address Translation (NAT) is another very commonly found security device in data networks. NAT works by showing a single IP address to Internet traffic and hiding all network nodes behind it. This is very much like a situation where all mail comes to your office with only the office's address, and the mail clerk distributes it to individual persons. NAT is similar to the office clerk. NAT makes a network secure by hiding individual machines and allows organizations to use a single public IP address, but when NAT is used on a network where VoIP is also expected to work it introduces enormous complexities into the system because all incoming calls end up coming only to the NAT server.

Competing Protocols

VoIP standards are not yet universally accepted. Primarily, there are two competing standards – H.323 and Session Initiation Protocol (SIP). Both these protocols have considerable market support, although SIP appears to be gaining ascendency. Due to the presence of two

protocols, vendors often tend to build in support for both in their equipment. Security needs are different as well and this is one aspect that purchasing managers must discuss carefully with their telecommunications staff. A conscious decision needs to be taken keeping a large number of factors in mind. If your deployment is going to cross country borders, then this needs even more careful study.

Besides H.323 and SIP, there is Media Gateway Control Protocol (MGCP) that is used to communicate between separate VoIP systems. MGCP is complementary to SIP or H.323 and provides support for multi-party conferencing and multimedia.

Due to differing protocols and related issues, designing and running a VoIP network over a busy, mission critical data network is something that is best left to experts. Implementing security in such an application stack is not for the faint hearted!

Every implementation will have its own peculiarities. You simply cannot have a 'one size fits all' solution. Every organization has to study its existing network and communication needs carefully before proceeding with a final solution. With this short background into VoIP peculiarities, we can now move to specific security threats.

VoIP Threats

Security threats to VoIP systems can be broadly broken down into three classes of threats. These cover areas of availability, confidentiality and integrity.

Attacks on Availability

Availability refers to the VoIP service being available for use when needed. Just as data networks, VoIP services are susceptible to a denial of service attack. In such attacks, the attacker attempts to prevent your use of the VoIP system.

There are several ways in which this is accomplished – one way is to send so many connect requests to a user that the victim is unable to connect to another user that its needs to talk to. Such kind of distributed denial of service attacks can come from anywhere on the Internet. There are other variations to this theme. In another version, a cancel message is spoofed so that as a victim is unable to build a connection with the other party. As soon as a connection is established, a GOODBYE or a cancel signal is sent.

There is a possibility of a physical attack as well. Unlike traditional telephones that operate using a 48 volt supply carried by the telephone

cable itself, VoIP systems need external power supplies. There could be many places where the power supply to components of a VoIP system could be disrupted. If the attacker chooses a critical switch correctly, he could disrupt major portions of your VoIP network.

To counter denial of service attacks, the key is to have strong authentication and sensible security such as shutting down of unnecessary ports etc. The VoIP firewall has to be set to reject unwanted traffic. Normal traffic statistics should be known so that abnormalities are detected early. All routers have built in traffic analysis software such as SNMP (older systems) and Netflow (new systems) that allow detailed traffic monitoring. These should be used to monitor traffic through your systems.

To handle physical threats, organizations need to implement strict security procedures, restrict areas that visitors can go to, implement access controls and provide guards. Redundancies of power supply and adequate back up generation capability needs to be ensured. Regular tests of your power supply systems are necessary.

Confidentiality Threats

Good confidentiality rests on the premise that information should not be accessed by individuals not authorized to receive it. This includes IP addresses, documentation, passwords, content, conversation history, and so on. Eavesdropping of unprotected VoIP conversations is easier because there are a large number of nodes between two users and any of these can be used to access the IP packets that form the conversation. A large number of free and paid tools are available that allow VoIP packets to be converted to audio files. These audio files can be saved and played back later at leisure.

Researchers have also shown[1] that certain VoIP phones and devices have a large number of undocumented ports and services. These can be easily found by competent attackers and used to eavesdrop on conversations. Many in-built systems for billing, call management etc. ship with default passwords that are well known to the VoIP community. Many of these issues can be corrected by simple and sensible administration. A well thought out security policy is essential to ensure that all default passwords are changed; unessential services are shut down and so on. Encryption protocols such as IPsec and SSH must be used to protect data packets so that even if an attacker gains access to network components, he is unable to understand the content.

Integrity Threats

There are a number of integrity threats to the VoIP network. Caller ID spoofing is probably one of the best known. In a number of well-known attacks,

[1] Shawn Merdinger, ACT P202S VoIP wireless phone multiple undocumented ports/services

attackers have been known to call up agencies such as Western Union and used a stolen credit card and a spoofed caller ID to order cash transfers[1]. Spammers also use these techniques to create attacks where they pose as banks or other trusted entities. Other integrity attacks rely on replacing a genuine client's information with that of the attacker. This will cause the call to be routed to the attacker. In a situation where the called party is not personally known, this could bring obvious benefits to the attacker – a scenario could be an attacker impersonating the help desk of a credit card company.

Other integrity threats arise from techniques known as **Registration Hijacking**, **Proxy Impersonation** and **Call Redirection**.

In **Registration Hacking**, the attacker alters the registration details of the victim and inserts his (the attacker's) details instead. This will cause all calls for the victim to be routed to the attacker. A denial of service attack on the victim during this period ensures that the victim cannot attempt to re-register. During this period, the attacker can assume the VoIP identity of the victim.

Proxy Impersonation tricks the victim into communicating with a rogue server instead of the regular proxy server. Generally, in VoIP communication, the proxy server is used to channel calls. If this server address can be replaced by a rogue server, all communication will be through the rogue server which will allow a number of attacks to be carried out.

Call Redirection is a development on the Proxy Impersonation. The redirected call can be passed on a route of the attacker's choosing and allows the call to be recorded. If a classic man in the middle attack is developed, then the entire conversation can be heard even if encryption is used. This is complex to do and one would only expect to find such attacks to be mounted on selected very high value targets.

There is no simple method to prevent caller ID spoofing on which the entire series of Integrity Threats rest. Experts say that the best thing to do is not to trust caller ID display without other supporting evidence. Strong encryption schemes help and administrators must take care that all VoIP software is kept updated and patched at all times. There are a number of VoIP vulnerability scanning tools which must be used regularly to test your installations.

Security Guidelines for VoIP Systems

With the above background, one can move on to the most useful security precautions that must be taken. These are discussed briefly in this section.

[1] http://www.schneier.com/blog/archives/2006/03/caller_id_spoof.html

Work from a Well-Designed Network Architecture

It makes sense to logically separate the data and voice segments of the network. This logical separation allows each type of bit stream to be handled optimally. The voice gateway must have strong authentication mechanisms in place and firewalls must be configured to handle voice correctly.

Use VoIP-Ready Equipment

As may be clear from the discussion earlier, VoIP systems have different characteristics from pure data. VoIP aware equipment handles VoIP traffic more securely and ensures better QoS than regular routers and switches.

Avoid Using Softphones

These are simple headphones that attach to a PC and use software to provide VoIP services through the PC. While such a setup is very easy to implement, this brings in a number of vulnerabilities. Viruses, worms and Trojans are very common on PCs connected to the Internet and these could open up your VoIP system to a number of threats.

Implement Strong Physical Security

If an attacker is allowed physical access to devices, he can perform a number of attacks or disable the system completely. Even if encryption is used and the contents of the call cannot be deciphered, much information can be gleaned from an analysis of traffic patterns. Good physical security needs to be implemented to control access to VoIP components.

Pay Attention to Power Back Up Systems

Adequate power backup must be provided to all VoIP components. Systems must be tested and UPS timings have to be checked out periodically. As mentioned earlier, a denial of service attack could be carried out by simply interfering with the power supply.

Patch Systems Regularly and Use Appropriate Antivirus Software

Any vulnerability in the operating systems, VoIP software and in the servers could give an opening to an attacker. Administrators have to ensure regular patch management. Viruses and worms are still a very major threat to any software based system, VoIP servers are not an exception.

Use Encryption

Even simple encryption protocols give a degree of safety. Transport layer security is the preferred method.

Conclusion

Even as VoIP is becoming an integral part of the corporate communication suite, many administrators make the mistake of being satisfied by providing VoIP components the same security as they do to their regular data networks. This is a major mistake. VoIP has very different system and security requirements as compared to other applications. Unless specific measures are taken, quality of service will always take a hit and system vulnerabilities will render the VoIP system unreliable.

A good implementation will logically separate the data network from the VoIP network. This will allow each to be optimized and provide the requisite security. While VoIP gives enterprises considerable new capabilities, ensuring secure and reliable communication in the face of hostile threats will need a planned and layered defense – all the way up from physical security to strong authentication and encryption.