Global Information Assurance Certification Paper

VoIP Security in Small Businesses

Version 1.4 b Option 1

Klaus Steinklauber
Date: May 15, 2003

VoIP Security in Small Businesses

Abstract

This paper reviews some of the security issues of VoIP (Voice over IP) in relation to the Small Business. The security requirements and implementations vary to a certain extent in how it is perceived and implemented in the Small Business enterprise in relation to the larger Corporations. A brief overview and recommendation of VoIP security issues are outlined.

Background

Voice over IP (VoIP) is a method of transmitting Voice signals over an IP network, also known as a packet network, instead of the Telephone Company's switched network [11]. It is becoming more and more prevalent in the world because vendors have mature products and increased capabilities and customers are trying to reduce costs [2]. With the introduction and boom of the Internet, Small Businesses realized that they had an opportunity to compete on a more even keel with large enterprises, because with the Internet you can reach the same audience that previously could only be reached by national TV commercials at extreme high costs.
This revolution is now happening again in the Phone industry that allows a Small Business to appear larger and can have presence in different geographical locations without incurring in long distance charges by using the Internet to access remote home workers and/or branch offices without the expensive Branch Office costs. Operational costs can be better controlled and cheaper labor costs can be tapped by using VoIP and the Internet. Some of the features of VoIP are:

- IP Phones or Internet telephones
- Inter-office trunking over the corporate Intranet or Internet
- Remote access from branch or home offices to both the voice and data networks via the Internet
- Internet call center access

Internet aware telephones have an Ethernet NIC (Network Interface Card) incorporated and come in several flavors, from specific hard IP phones to soft-phones or PC-phones. Soft or PC phones are a combination of software and the hardware of a PC. It is not necessary anymore to have a dedicated phone line or a telephone set, you just need an Internet connection fast enough to make a VoIP call. Popular software programs like Messenger from Yahoo and Microsoft are a couple that can make telephone calls from your PC using a microphone and speakers/headsets plugged into an Audio Card [13].

The first implementations of VoIP have been using the inter-office Data circuits to carry the phone traffic, thus reducing long distance charges especially for offshore remote sites [8]. In this situation a company already had a leased line to be used for their Data network or had spare capacity. Even before the Internet exploded, large Corporations were using Time Division Multiplexing to combine Voice and Data over the same circuit, although the voice quality was poor. The further away the remote site is the more savings will be realized.
With the Internet and applications rewritten to be accessed via a browser allow people in customer service and other positions to work from home, thus creating the SOHO (Small Office Home Office) industry. Company customers need to contact the employees without giving out new phone numbers and confusing the customer, making the relationship totally transparent. Use of VoIP allows these employees to use a single broadband Internet connection to be used for Data and Voice access to their company resources.

The Security issues

Reviewing the security aspect of VoIP we are facing several problems, one related to the underlying Protocols and the second with the Operating Systems that the Manufacturers are using to run their VoIP services. Another factor is the human factor and the culture surrounding the Telephony issues [13].
In the past, with the large Telco's monopoly the user did not have to worry about the provisioning, installation and maintenance of their Telephone system, thus creating a sense that the Telephone problems did not belong to the user. The result of this attitude sometimes resulted in surprised huge costs from Toll fraud and abuse by employees. With the advent of VoIP the situation has changed and the responsibility lies with the Small Business to plan, secure, implement and maintain their VoIP and network infrastructure. The benefit is a faster response to move add and changes and the reduced cost directly associated with this responsibility.
The majority of VoIP users that are vulnerable are the Small Business's users, because they rely more on outside vendors and/or their technical staff has limited knowledge. The emphasis on controlling costs and fierce competition is met with more integration which translates in an apparent lower investment for the infrastructure by either combining the Network infrastructure for Data with the Voice portion and/or using the File Server as the foundation for the PBX (Private Branch Exchange) application.
On top of these technical issues is the person in charge for the maintenance and support of the combined network.
What experience should that person have?
Should the Small Business outsource the service to the supplier, reseller or consultant?
Should it use a combination of in-house and outsourced services? What knowledge, experience and certifications should the service person posses?

There are two kinds of attacks possible to a network – external and internal. For example in a VoIP network, external threats are attacks launched by someone that is not a participant in the message flow during the VoIP based call. External threats usually occur when the voice packets traverse an untrustworthy network and/or the call traverses a third party network during the message transfer [10]. The internal threats are much more complicated to detect because it usually involves an internal VoIP participant, because when an internal VoIP participant launches an attack, the trust relationship is defied. These types of attacks are not only limited to VoIP but are applicable to Data networks as well.

Security vulnerabilities

As mentioned before, we have two vulnerabilities one that is dependent on the protocols used in VoIP implementations and the other is related with the operating Systems involved. Each protocol or service has its own security vulnerabilities depending on which protocol SIP, H323 and MGCP is used. We can generally classify the types of vulnerabilities as follows:

- Protocol vulnerabilities
- Infrastructure vulnerabilities
- Operating Systems vulnerabilities
- Human vulnerabilities

Protocol vulnerabilities

The Protocol is the underlying mechanism to perform and allow the transfer of intelligence over the network. The protocols used are base on standards that governing bodies like the ITU, IETF, IEEE and others regulate. This paper will briefly discuss the following standards [3]:

- H.323 from the ITU, which was first approved in 1996 but had its beginnings in the early 1990's.
- Session Initiation Protocol (SIP) from the IETF, which was first, approved as an RFC (2543) in 1999.
- MGCP was first published by the Media Control Working Group as RFC (2705) in 1999.
- H.248/Megaco is an ITU recommendation that define "Gateway Control Protocol". It's a joint collaboration between ITU and IETF. H.248 is based on and extends MGCP.
- RTP Real-Time Transport Protocol also known as IETF RFC (1889) is a transport Protocol for real-time applications and is used by all VoIP signaling Protocols

The protocols are divided into signaling or call setup and the transport protocol, which is RTP. MGCP is a combination of two other protocols: IDPC (Internet

Protocol Device Control) and SGCP (Simple Gateway Control Protocol). A basic difference between these three architectures is where intelligence is concentrated [8]. SIP places most of the intelligence at the endpoints whereas MGCP places the intelligence in the network components. H.323 places intelligence everywhere and is a comprehensive protocol, which tries to address all aspects of a VoIP system. It is an umbrella system, which includes a number of other specifications such as:

- H.225 - call control signaling, registration and admission
- H.235 - security issues: Authentication, Integrity, Privacy and Non-Repudiation
- H.245 - channel usage negotiation
- H.261 - Video Codecs
- G.723 and G.729 - Audio Codecs

A H.323 system is composed of four main components:

- Terminal – End user equipment that supports Voice/Data and Video
- Gateway – Interconnects two different networks, PSTN to/from IP
- MCU or Multipoint Control Unit – Allows conference with multiple Terminals at the same time
- Gatekeeper – Performs authentication services to Terminals

SIP is a less complicated protocol and hence, some would argue, more flexible [3]. It is a challenge-response based system similar to the HTTP protocol [4]. The main components of a SIP based systems are:

- User Agent Client or UAC – Responsible for the initiation of a call by sending an URL
- Proxy server – Responsible for the routing and delivery
- Redirect server – Has a user database that informs proxy servers about the users location

The most common types of VoIP attacks are as follows:

Denial-of-service attacks (DoS): Prevention of access to a network service by bombarding servers, proxy servers or voice-gateway servers with malicious packets

Eavesdropping: Unauthorized interception of Voice packets or Real-Time-Protocol (RTP) media stream and decoding of signaling messages

Packet spoofing: Impersonating packets or person transmitting information

Replay: The retransmission of genuine session so that the device receiving it reprocesses the information

Message integrity: Ensuring that the message received has not been altered during transit

As can be noted, using the protocols for VoIP weaknesses, which also apply to Data networks, one can perform all the above attacks.

Infrastructure Vulnerabilities

VoIP networks can be safely deployed in a secure isolated network environment without too much of a risk. This applies to all protocols, but the reality is that the enterprise needs to be connected to the Internet especially in a global commerce environment as it is today. We not only have to worry about securing our Data network but we must also secure our Voice network. One mayor concern is that of availability of our networks.
Whenever an outage occurs with our Data network we are still dependent on our Voice network as a form of backup to our Data network. By combining our Voice and Data network the pressure for availability increases dramatically. Every Businessman will immediately switch to the Telephone in order to continue operation, with at least the first call being made to their service technician or support person, either in-house or external [15].
This situation creates an environment that could become very appealing to attackers. By using denial of service attacks DoS, for example, it becomes very easy to disrupt two services instead of only one, which malicious hackers or script kiddies could exploit very easily if not protected against it.
In classical telephony networks we have similar attacks like Eavesdropping, frequency flooding, fraud and impersonation. Some of these are easier then in the digital IP network and others require more sophisticated equipment. The more impacting attacks against the PBX are the toll fraud attacks, which in VoIP would be equivalent to the server or Call Manager attack. In VoIP the problem of eavesdropping is much larger then in the classical telephony network due to the fact that all conversations travel over the same network whereas in the classical case the attacker needs access to the individual telephone pairs and then it would only capture the calls from that individual line. That is the reason why it is so important to use switches instead of hubs. Since more and more calls will be made over the Internet, the issue of firewalls becomes a real one. Again, since the amount of devices on a network is small, usually a DSL connection is sufficient. Manufacturers have produced network equipment that is inexpensive and at the same time have a hub, router, DSL and firewall all incorporated in a single unit. These firewalls have been designed for Data networks and not for VoIP services. If the firewall function is not integrated into the DSL/router box than usually an inexpensive software firewall is used for the PC's, but this firewall does not protect the VoIP hard telephones leaving them exposed, although the

phone manufacturers are trying to incorporate security into their devices. In recent polls H.323 is the prevalent protocol and it uses UDP to make and establish the connection amongst two Terminals, this means that the firewall needs to open a series of ports in order for the VoIP communication to function properly. Since being a Small Business it cannot justify using private circuits for their remote offices, they use the Internet for that purpose and therefore use an insecure link.

Operating Systems vulnerabilities

The majority of Operating System vulnerabilities are buffer overruns that allow an attacker to take partial or full control of the host machine. These are not the only ones and they vary by Operating System manufacturer and versions [12]. They are mostly related to lack of security in the initial development phase of the Operating System and therefore are discovered after the launch of the product.

Human vulnerabilities

In this category we have the problem of the Network Administrator and the Management of the enterprise. There is a battle between the easy of use and the security of a network. In a Small Business environment the problem is compounded because a few people use several hats in order to control costs and because there is not enough fulltime work for one position only. The other problem is the cost of a fulltime person with a lot of experience and to circumvent this the enterprise relies heavily on outside consultants, resellers and/or installers. In this situation the tendency is to leave the decision over security issues to that consultant or reseller which does not have a great incentive to spend extra time to secure and maintain the network unless he is specifically contracted to do it.

Recommendations for securing against attacks

One of the first considerations that should be made is that one must view the VoIP network in the same way as the traditional Data network from the security perspective. The basic steps and standard guidelines to protect a Data network apply to the Voice network as well.

Physical protection:
Every network and wiring closet should be protected via access control devices and surveillance equipment. This is one area that in Small Business's is most overlooked and not taken into consideration. The general attitude is that since we are so small and everybody knows everybody we do not need to make the additional investment. One can find the server and switches in the manager's office or in the copier/filing room where everybody has access. This exposes the

network to the internal attack threat from a disgruntled coworker or by mistakes due to lack of knowledge.

Restricted access:
One should disable all Telnet access or at least restrict it to one or two devices within the network. The use of TACACS+/ RADIUS authentication servers should be used for all devices to avoid the use of sticky notes with passwords written on it for everybody to see.

Network restrictions:
Disable all unnecessary services like HTTP, TCP/UDP small services, Finger, RSH/RCP, etc. Use switches and implement VLAN's to separate your Data devices from your VoIP devices. Avoid using soft or PC Phones on the network due to the potential Operating System vulnerability of the PC. Never use VLAN 1 for your VoIP network and Call Manager server, because this is the default VLAN on all switches.

Secure Ethernet Switches:
In order to better secure the network it is essential to use a switch and implement VLAN to separate the different networks. There should be a VLAN for every network, one for Data users, one for VoIP users and one for network trunking. On the VLAN assigned to network trunking there should be no users connected and all unused ports shall be member of a non-routed separate private VLAN.

Firewall:
Older and low cost firewalls are lacking the capability to protect networks that use VoIP [5]. These firewalls have to open a range of UDP ports in order for the VoIP services to work thus creating a major security risk. The solution available is to use Voice aware firewalls and/or Voice proxy firewall that can perform state full inspection and open ports when needed and close them after use [7][9].

Operating Systems:
All the VoIP services run on Operating Systems like Windows NT/2000/XP, VxWorks and IOS amongst others that are susceptible to attacks that can allow an intruder get access and compromise the systems. Therefore it is essential that these Operating Systems are being patched and maintained up to date and have all unnecessary services turned off.
As an example of an Operating System buffer overflow is the one found in 3Com's NBX IP Call Manager "*The 3com NBX uses VXWORKS Embedded Real time Operating system and what appears to be their own internal ftp server. This buffer overflow problem seems to be one similar to the AIX ftpd reported in CVE 1999-0789 and has been assigned bugtraq id 6297*". The full details can be viewed at the following URL "http://archives.neohapsis.com/archives/vulnwatch/2003-q2/0045.html"

Eavesdropping:

To avoid the possibility of the information of a Voice packet being intercepted encryption should be implemented so that the attacker will be unable to understand what was said during a given conversation. In this area Ipsec, secure RTP and VPN are alternatives to protect the information from unauthorized call participants.

Antivirus:
Every system should be protected against Virus attacks. With the different types of Operating Systems this can be a major problem, especially if one wants to centralize the administration and automatic distribution of Virus definition files. Nevertheless Antivirus software should be installed on all systems, no matter how complicated it will be. A virus attack can be more costly then the cost of an Antivirus software implementation.

Back-up:
The back-up issue gets quite complicated as well especially in cases where different Operating Systems are involved in a VoIP deployment. Some of the back-up software solution has not the appropriate agents to centrally back-up the Data, so they either do not back-up. Some of the vendors of VoIP products have a built in back-up functionality in their product. A law enforcement issue can arise with regards to retention of the call records for legal incidents besides the issue of claims and forensic, and therefore a back-up of these CDR (Call Detail Record) records is a must.

Reseller/installer:
A great deal of consideration in the selection of the reseller and/or installer has to be made, because otherwise in the integration of the two networks a weakness could be introduced by the reseller and/or installer because of his experience usually in only one network, either Data or Telephony. This creates the danger that they do not understand all the security risks of both types of networks. Everybody is striving to obtain the least expensive product, but that can also lead to some mistakes in the design not necessarily due to lack of knowledge but rather due to the traditional Data network design guidelines. For example, you have a 15-employee organization that needs a telephone and a computer for everybody, but 5 employees work from home. So the total telephones at the office will be 10. On a low traffic network the standard design guidelines for a network of this size are to use a hub instead of a switch. The reseller and/or installer will recommend the use of a hub because he knows that if he does not, his competitor might and under price him. The other situation is that a Small Business already has a data network and a legacy phone system but now it needs to expand to remote sites and therefore sees the opportunity to remove the legacy phone system because the savings will pay for itself and new features like voicemail, will be a bonus. Now, the existing Data network has a hub, but since the office is very small it is left without change because that is one less expense for the expansion.

Ongoing Security issues

Policy and Procedure
A policy should be implemented outlining the minimum installation configuration, like using switches instead of hubs. Also it should be outlined how maintenance should be performed and what documentation shall be required as well as who is responsible for the back up, amongst other items. What users are allowed to use and what needs to be done if a policy is broken?
When considering implementing VoIP in a Small Business it is of the utmost importance to request from the reseller and/or installer a plan on how the updates, patches and support will be handled once the system is installed. The price of the implementation is important, but more important is that the right infrastructure is implemented in regards to network security.

Other emerging VoIP services

In an effort to provide new services and revenues the ISP's (Internet Service Providers) are starting to implement VoIP services. These services are known as IP Centrex or Virtual PBX [6][11]. These services allow the ISP to act as a Telephone Company Centrex service for their customers but at a much lower rate and with more features. Some of the issues with this type of service are that it uses the SIP protocol together with public IP addresses. This exposes the internal network that is behind a firewall to open up the firewall for this public address in order to be able to use VoIP. Firewall vendors are creating Proxy firewalls that will translate from a public IP address to a private one. These firewalls would be deployed at the ISP facilities. This creates some security, but will not protect from other customers of that particular ISP from being attacked.

References.

1. "SIP: Session Initiation Protocol" RFC # 2543
   URL: http://www.ietf.org/rfc/rfc2543.txt?number=2543
2. Verrinder, Karen "Long-Awaited Voice over IP Growth Is Slowly Approaching Reality in IP PBX Markets" April 23, 2003
   URL: http://www.probegrp.com/press%20releases/2003/vopm03v4n1.pdf
3. "Standards" accessed February 27, 2003
   URL: http://www.protocols.com/voip/standards.htm
4. White Paper "Security in SIP-Based Networks" accessed March 29,2003
   URL:
   http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml
5. Lee, Stephen "Vendors eye VoIP Security" InfoWorld January 10, 2002
   URL: http://www.nwfusion.com/edge/news/2002/0110voipsec.html

6. Shook, Laurie “Virtual PBX: The Inevitable Shift for Business or Here Comes IP Centrex”
URL: http://www.vocaldata.com/pdf/071602/Virtual_PBX_IP_Centrex.pdf
7. “The Voice Proxy Firewall Provides an Integrated Security Solution for IP Telephony Service Providers” VocalData Ver 2.0 December, 2002 URL: http://www.vocaldata.com/products/Voice%20Proxy%20Firewall%20White paper%202.0.pdf
8. Marjalaakso, Mika “Security Requirements and Constraints of VoIP”
URL: http://www.hut.fi/~mmarjala/voip
9. Briere, Daniel and Gage, Beth “Can we talk? VoIP’s Firewall challenges” The Edge June 11, 2002
URL: http://www.nwfusion.com/edge/columnists/2002/0625bleeding.html
10. Vivek, Subha “VoIP Security: Is Anyone Listening?” January 16, 2002
URL: http://www.infosecnews.com/opinion/2002/01/16_04.htm
11. Bakke, Steve “VoIP Security Challenges In Enterprise And Service Provider Networks” November 2002
URL: http://www.tmcnet.com/it/1102/1102voc.htm
12. Scheidell, Michael “[VulnWatch] 3com NBX IP Phone Call manager Denial of Service – Update” April 27, 2003 URL: http://archives.neohapsis.com/archives/vulnwatch/2003-q2/0045.html
13. Vijayan, Jaikumar “VOIP Security on the Back Burner” October 7, 2003
URL: http://www.computerworld.com/securitytopics/security/story/0,10801,74778,00.html
14. Hockmuth, Phil “Costs, security vex VoIP users” February 24, 2003
URL: http://www.networkworldfusion.com/news/2003/0224voicecon.html
15. Carr, Kathleen and Duffy, Daintry “The Pitfalls of VoIP” December 2002
URL: http://www.csoonline.com/read/120902/briefing_voip.html

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS