

VoIP for SMBs – Should You Worry about Security?



Secure Computing® is a global leader in Enterprise Gateway Security solutions. Powered by our TrustedSource™ technology, our award-winning portfolio of solutions help our customers create trusted environments inside and outside their organizations.

Table of Contents

Introduction	2
VoIP Protocols.....	3
Growth Rate of VoIP	3
Reasons for Rapid Growth.....	4
Benefits.....	4
Concerns and Converged Services.....	4
VoIP Security Threats	5
Peer-to-Peer VoIP	5
Is the VoIP Threat Real?.....	5
Basic Security Goals	6
Confidentiality.....	6
Availability	6
Authentication.....	6
Access Control.....	7
Integrity.....	7
Types of Threats.....	7
SPIT.....	8
Vishing	8
Eavesdropping.....	8
Spoofing.....	8
Solutions Available.....	9
Best Practices	9
Strategy of Isolation.....	10
SnapGear Solutions.....	10
Unified Threat Management	10
TrustedSource.....	10

Secure Computing Corporation

Corporate Headquarters

4810 Harwood Road
San Jose, CA 95124 USA
Tel +1.800.379.4944
Tel +1.408.979.6100
Fax +1.408.979.6501

European Headquarters

Berkshire, UK
Tel +44.0.870.460.4766

Asia/Pac Headquarters

Wan Chai, Hong Kong
Tel +852.2598.9280

Japan Headquarters

Tokyo, Japan
Tel +81.3.5339.6310

Brisbane, Australia Headquarters

Tel: +61.7.3435.2888

For a complete listing of all our global offices, see www.securecomputing.com/goto/globaloffices

© 2007 Secure Computing Corporation. All Rights Reserved. SNAP-WP-Jun07vF. Secure Computing, SafeWord, Sidewinder, Sidewinder G2, Sidewinder G2 Firewall, SmartFilter, Type Enforcement, CipherTrust, IronMail, IronIM, SoftToken, Enterprise Strong, Mobile Pass, G2 Firewall, PremiseAccess, SecureSupport, SecureOS, Best, Cyberguard, SnapGear, Total Stream Protection, Webwasher, Strikeback and Web Inspector are trademarks of Secure Computing Corporation, registered in the U.S. Patent and Trademark Office and in other countries. G2 Enterprise Manager, SmartReporter, Security Reporter, Application Defenses, Central Management Control, RemoteAccess, SecureWire, TrustedSource, On-Box, Securing connections between people, applications and networks and Access Begins with Identity are trademarks of Secure Computing Corporation.

Introduction

Voice over Internet Protocol, or “VoIP”—transmission of voice packets over IP networks—is one of the most innovative emerging trends in telecommunications. Despite the fact that the Internet was not designed to carry voice traffic, technologists have quickly stepped up to the plate to make this new application possible. And the state of the art has advanced quickly, with VoIP moving from low-quality, clunky connections, to a high-quality, low cost, viable alternative to the Public Switched Telephone Network (PSTN).

From the first transatlantic cable, the telecommunications industry has experienced multiple significant revolutions. The rapid, mass adoption of the Internet not only changed the telecom industry, it changed the entire world. The Internet brought widespread usage, market-driven data convergence, and a whole new world of e-commerce. Ubiquitous Internet access has also expanded beyond data, to include voice- and video-based IP networks. Today, VoIP has brought many benefits; besides high efficiency and low cost, it continues to revolutionize the entire telecommunications industry.

VoIP, as a key component of this revolution, has gained attention from the general population as a useful, convenient and relatively inexpensive service; and mass deployments of commercial VoIP service has been rolled out to consumers and businesses alike, by startups and competitive carriers, as well as incumbents who have had to revisit their traditional service models. In addition, VoIP has gained the attention of scientists, researchers, analysts, and entrepreneurs as they delve deeper into looking at the potential security challenges that VoIP poses now and will pose in the future as it gains further acceptance.

With the convenience of this new model of communication comes a new set of security vulnerabilities and concerns, both in technology and policy. VoIP transmits bits of voice conversations contained within data packets over IP-based networks to reach the end-user, often combining transmission over the PSTN with transmission over the Internet. As such, it inherits security vulnerabilities from the PSTN, IP networks, and from the many new messaging applications that VoIP makes possible. Many VoIP security issues are similar to traditional messaging security concerns, such as unwanted messages (or calls) and the potential of DDoS attacks that consume bandwidth and affect quality of service (QoS). With the merging of voice and IP, QoS for voice connections becomes a function of overall network QoS. Other concerns include privacy—are calls treated as data files if delivered via IP? And if they are, will those files be subject to recent regulations that govern some data? What technologies can be adapted from the email and instant messaging world to protect VoIP? What new technologies may be required to fill any gaps?

VoIP for small- and medium-sized businesses, and the security necessary to deploy it to those businesses, is a particularly vexing problem. VoIP first appeared as proof-of-concept experiments, and was used by “power user” individuals who talked directly over computers. The voice quality was shaky and jittery, there was delay, and the interface was awkward, but it was nonetheless an exciting application that held great potential. Improvements in call quality and the appearance of special VoIP phones and equipment soon took VoIP to the enterprise, where large companies used it to connect branch offices. It was not until later that VoIP matured to the point where it was affordable and intuitive enough for small- and medium-sized businesses to also gain some advantage from it.

This paper outlines the landscape of VoIP in telephony history, presents an outline of prevalent VoIP protocols and then explores the current security vulnerabilities in VoIP. Finally, a discussion of solutions to VoIP security vulnerabilities is presented. We leave to future work the discussion of modifying current messaging security technology to better address VoIP security vulnerabilities as well as new techniques designed specifically to protect VoIP.

VoIP Protocols

VoIP provides an entirely new method of transmitting voice packages. It utilizes the advantage of packet-switched networks by converting voice to data packets and transmitting the data packets over the Internet or through any other IP-based network. It promises a key technology to complement and potentially replace traditional circuit-switched PSTN, or older first generation packet-based voice technologies based on Frame Relay or Asynchronous Transfer mode (ATM), with a packet-based network that provides better QoS with higher efficiency and lower cost. However, the benefits of using VoIP come at a cost.

To understand VoIP security concerns, first we need to understand the VoIP system. Any discussion of VoIP should start with a discussion of signaling components. The heart of a VoIP architecture model of PSTN gateway is Media Gateway Controller (MGC). The MGC receives signaling information from the media gateway and instructs it to alert the called party in order to establish, modify and destroy connections with its peers within a network. The MGCs interact with each other via signaling protocols. There are two standardized intelligent protocols: H.323, and SIP (session initiation protocol). Both are widely recognized standards used throughout the industry, and promoted by recognized standards bodies. H.323 is promoted by the International Telecommunication Union (ITU), and SIP from the Internet Engineering Task Force (IETF). The standards do not compete with one another, and the standards bodies' goal is to establish common technological ground among all members. The IETF is a community of individuals and companies that are concerned with the evolution of the Internet architecture and the smooth operation of the Internet; and ITU is an agency of the United Nations which recommends standards to be used in communications technologies.

H.323 is not an individual protocol, but rather a complete, vertically integrated suite of protocols that defines every component of a conferencing network: terminals, gateways, gatekeepers, MCUs and other feature servers. All of the protocols—dozens of back-and-forth messages—must be negotiated to set up a simple point-to-point voice call. SIP is an application-layer control (signaling) protocol for creating, modifying, and terminating sessions with one or more participants. SIP does suffer from NAT or firewall restrictions. The NAT router may be able to handle the signaling traffic, but it has no way of knowing that the audio traffic is related to the signaling and should hence be passed to the same device the signaling traffic is passed to. As a result, the audio traffic is not translated properly between the address spaces.

There are also some proprietary VoIP protocols, the most popular of which is Skype. Skype operates on a peer-to-peer model rather than the traditional server-client model. The Skype user directory is entirely decentralized and distributed among the nodes in the network, which means the network can scale very easily to large sizes. Since Skype is a proprietary protocol, the security vulnerabilities are less obvious, but are nonetheless present. The greatest vulnerability with Skype and other proprietary peer-based protocols is that individual users will install them on their own, without permission and oversight from IT, opening up a possible “back door” to the network and making it difficult to keep control over policy and security. Skype carries with it several inherent risks not posed by other commercial VoIP systems, and because it does not use standard VoIP protocols, it makes it easier for malware to be carried along with voice packets. Most corporations prefer to block these peer-to-peer VoIP systems, and this can easily be done with a tool such as Webwasher® from Secure Computing®.

Growth Rate of VoIP

The North America small and medium business segment for hosted business-VoIP is set to reach US\$416 million in 2007—from about US\$165 million in 2005. Between 2005 and 2010, the cumulative growth rate will cross 56.9%, according to the latest study by AMI Partners Inc.

In addition to the business segment, VoIP has entered the residential market in a big way, particularly with large telecoms rolling out “triple play” offerings that deliver cable television, broadband Internet, and telephony, all in one.

Reason for Rapid Growth

Cost savings is certainly one of VoIP's key drawing cards. A recent Intel study estimated that a medium-sized company could cut costs by up to 52% a year over a traditional PBX (Private Branch eXchange) system. In the consumer market, the availability of the triple play is another reason for growth; this attractive offering delivers the advantage of single billing and cost savings, while bringing carriers more average revenue per user (ARPU) and less churn.

A primary indicator of this growth is the acceptance of IP Centrex solutions, especially in the SMB marketplace; and today, most SMB organizations that are installing new Centrex solutions start out with an IP-based system. Centrex, popular especially with small and midsize businesses, is easy to maintain because the equipment is owned and operated by the service provider, and located on the service provider's premises. In an IP Centrex system, the customer transmits voice calls to the network as packetized streams over a broadband connection. The greatest advantage of IP Centrex over traditional Centrex is that with IP Centrex, a single broadband connection can carry multiple simultaneous calls, whereas traditional analog Centrex, each telephone station needs a separate pair of copper wires.

These systems offer many advantages for businesses of all sizes, because they are able to deliver not only the same features of older Centrex services, but other value-added services as well that would not be available on a conventional Centrex. According to market research firm Compass Intelligence, IP Centrex is one of the fastest growing segments of the telecom industry, with double-digit annual growth projected through 2010. Solid growth of this market has also been enhanced by the entrance of mature vendors into the IP Centrex marketplace. In addition, in the PBX market, major vendors such as Cisco are also delivering IP-based product offerings specifically targeted at SMBs. Both IP PBX and IP Centrex solutions offer great cost advantages for companies, deliver value-added services that are unavailable in traditional solutions, and are easy to implement and manage.

Benefits

Because VoIP is software-based, users of it can enjoy new features that are not possible to deliver on a standard circuit-switched telephony system. These technological innovations bring new services to the consumer and business user, and greater revenue for the carrier, opening the door to a series of new features, such as audio and video conferencing, unified messaging, remote call management etc. The technology also provides tighter integration with a business' backend infrastructure, enabling voice and media integration into Web sites, email, messaging systems, and other enterprise IP assets.

Concerns and Converged Services

The advantages to VoIP are at the same time its disadvantages from a security viewpoint. The biggest "killer app" of the VoIP world is not the phone calls that go over IP networks, but the ability to have blended services.

The telecom industry, for decades, evolved very little beyond standard telephony service. The combination of deregulation, the advancement of the Internet, and an increasingly demanding and sophisticated consumer has changed all that. Today, consumers and businesses expect a lot more from their telecom provider. VoIP is only the beginning. Of course, it goes without saying that users expect VoIP service to be just as secure as switched circuit telephony, and so that's the first challenge. The second is to provide a continuing rollout of new complementary services. Technology such as IP Multimedia Subsystem (IMS) will play a big role in these services, giving carriers the technology to roll out a variety of data and multimedia applications that work with the VoIP system. These converged services may include things like integrated communications, impromptu conversations, and spontaneous collaboration; push-to-talk, multiparty gaming, videoconferencing, multiple messaging applications, and content sharing. Through the VoIP connection, users, especially business users, will also start to demand access to corporate data, email, an address book, and other useful related applications.

VoIP Security Threats

A VoIP system has multiple components, and therefore multiple attack targets. VoIP converts voice to data packets and sends them through networks, converts the packets back to voice and delivers to the end users via phones. The system incorporates IP networks, the PSTN, hardware such as IP PBXes and the phones themselves, and software messaging applications. More advanced systems may integrate with several other systems on the back end, such as databases, customer service applications that may contain sensitive customer information, and other messaging systems.

Each of these many components has certain security issues. The PSTN by itself does not carry such severe threats. Eavesdropping on a conversation, for example, requires physical access to the wires. Hacking a PBX is possible and has been done, but it requires highly specialized knowledge, and again, physical access. Similarly, “spoofing” a call on the PSTN is impossible. The telephone company provides the authentication function, which lets the recipient of a call know that whoever is calling, is who they declare to be. If your caller ID says that your Aunt Martha is calling, you can be reasonably certain that it is she.

Transferring phone systems to an IP network opens them up to many of the security concerns associated with Ethernet data networks, which were never a problem for simple PSTN calls. For example, IP-based networks are vulnerable to DDoS attack. In a VoIP system, a DDoS attack is especially dangerous, because it can bring an enterprise’s entire phone system down in a matter of minutes. In the messaging security world, spam and virus threats also stand out. Because VoIP covers all three areas (the PSTN, IP networks, and messaging), it inherits the security concerns from each of them.

Also, the fact that VoIP is just another data application from the network’s point of view has both its advantages and disadvantages. What this means unfortunately, is that attacks that are not specifically targeted at the VoIP network may nonetheless affect it.

Peer-to-Peer VoIP

Most businesses will deploy VoIP through special equipment, like an IP PBX, or through a managed service provider or IP Centrex service. Some SOHO companies and individual consumers may choose to implement one of the peer-to-peer VoIP services, such as Skype or Google Talk. It may also happen that within many companies, individual users may also deploy one of these peer VoIP systems on their own desktops without knowledge or permission from the IT department. This is a dangerous practice.

Many of these types of tools are designed to bypass the firewall whenever possible, and may introduce many vulnerabilities into the network, especially if they are unprotected and uncontrolled. The best strategy is for a company to block access to these services at the firewall level.

Is the VoIP Threat Real?

Even though many potential VoIP security vulnerabilities have been mentioned by analysts and the press, they are not yet a serious widespread threat. Currently, there is very little evidence of VoIP-specific attacks, but that’s only because attackers have bigger fish to fry. VoIP is growing at a phenomenal pace, and it’s only a matter of time before it becomes an attractive target.

Already, the first signs that hackers are turning their attention to VoIP are starting to appear, and the Voice over IP Security Association (VOIPSA) has published a list of tools that attackers can use to target VoIP applications. These tools are publicly available and easy to find. According to VOIPSA, VoIP hacker tools include sniffing tools which can analyze SIP traffic and listen in on conversations, as well as scanning and enumeration tools, and even packet creation tools, which can create phony SIP messages. Flooding tools are available to launch flooding attacks, and VoIP fuzzing tools can manipulate messages. Signal manipulation tools can disconnect an active VoIP conversation, reboot phones, or cause an incoming call to be rerouted to an attacker’s phone. VoIP media manipulation tools can take an audio file and insert it into an active conversation.

The threat is very real. On the email front and on the data network, viruses and other attacks were at first simple nuisances, but they have proliferated at an alarming rate, and the nature of these attacks has changed. Today, attacks are highly targeted, designed to cause large amounts of damage, and reap illicit profits. The threats to VoIP will evolve in a similar fashion—although the duration between “simple nuisance” and major threat will be significantly shorter, since attackers have already had a taste of success on the email front.

Basic Security Goals

Despite the variety of security concerns that each individual system carries, all of them can be categorized as follows: confidentiality, access control, availability, authentication, and integrity.

Confidentiality

Nobody wants his/her private conversation heard by a third party. In order to tap the PSTN system, physically accessing wires has to be involved. In an IP network, hackers can virtually break into anybody's conversation. VoIP systems transmit data encapsulated into discrete packages along the network path. While en route, these packets may pass through many servers and networks. Unauthorized parties could capture the packets and interpret them. The data might still get transmitted to the destination, but a copy of the data could be retained and replayed later. Confidentiality is one of the design goals for many cryptosystems, made possible in practice by the techniques of modern cryptography.

Availability

Availability means providing continuous service for intended users. In the PSTN, availability was ensured through network engineering and limited access to the network. For the most part, unless a tree knocks down wires during a storm, you have continuous service. With voice packets traveling through IP based networks, Denial of Service (DoS) becomes a serious problem. By attaching a PC to the VoIP network, it is possible to send malformed messages to a target phone or to cause a buffer overflow on one of several fields, resulting in a crash. Also, by performing any of these attacks on the switchboard phone, it has been shown that it would be relatively simple for an attacker to disable an entire phone system in minutes.

Availability could be interrupted when an attacker issues message flooding. For example, spammers could use an application to launch spam attack to a specific server. While all the bandwidth and CPU resources are consumed to process spam, the server cannot serve the legitimate uses any more. The same scenario could happen to VoIP traffic too.

Authentication

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Phone companies identify customers based on the line with which they are connecting to. PSTN is a wire and circuit switching-based system, and the telephone number serves as the identity. That means authentication of a receiver is limited to reliance on the correct routing of a call and authentication of a sender is restricted to the phone number of sender. It is rather difficult to spoof the telephone numbers. However, in VoIP, spoofing identity is much easier. For instance, plain text SIP messages are trivial to modify or inject, particularly over broadcast media. Although SIP is not encrypted, it can be protected using IPsec, SSL/TLS or S/MIME. However, even then, some header fields like “To” and “Via” must remain visible so SIP requests can be routed correctly. Attackers can thus send spoofed INITIATE requests containing phony IP addresses. Or an attacker who captures SIP setup messages can use spoofed “BYE” requests to disrupt calls in progress.

Access Control

Access control is the ability to permit or deny the use of a network by limiting the actions or operations that a legitimate user of a computer system can perform. Access control assumes that the authentication of the user has been successfully verified prior to enforcement of access control via a reference monitor.

For instance, in a peer-to-peer VoIP application, an audio stream is encrypted so that intermediate nodes cannot access it. The initiator of the conversation has to verify the state of the platform, including the client application and the audio output channel. That makes sure that in an end platform, an audio stream would not be illegally accessed by other applications or processes.

Integrity

Integrity ensures that the data received is the data sent. Since VoIP data packets go through many servers and networks, it's conceivable that packets could be tampered within the network, without being noticed by either end-user. For example, SIP signaling messages are sent "in the clear," which allows attackers to collect, modify, and replay them as they wish.

Types of Threats

Knowing that VoIP will likely be just as widely used, we want to remain ahead of the threat game and be armed with a comprehensive assessment of existing threats and solutions. VoIP security must not be overlooked. The major vulnerabilities of a VoIP system include:

- IP infrastructure
- Underlying operating system
- Configuration
- Application level

Types of possible threats include:

- Interception and Modification – Voice and data disruption
- Voice and data service threats – Eavesdropping
- Social Threats – Misrepresentation, Theft of Services and Unwanted Contact: SPIT, Phishing
- Rerouting calls to expensive sites. "Call Fraud" – re-routed to a premium number.
- DoS attacks to destroy networks. This could be a tangential effect if your VoIP network is running on the same network as your data. Could be targeted to VoIP applications too though.
- Interception of calls – though not considered one of the highest threats
- Unpatched firmware/VoIP applications. Same inherent security issues along with every other application you are running
- SPIM, SPAM, SPIT, Vishing, and Phishing

Although many potential VoIP attacks would allow for random mischief, it is likely that the bulk of attacks would follow the same pattern as other types of Internet attacks, and be centered around deriving illicit profit. The "low-hanging fruit" of illicit VoIP activity would probably be toll fraud, or rerouting of VoIP calls to premium or "900" numbers.

Even though VoIP security issues are not severe yet, it is critical to understand the importance of it and be well prepared. Email and spam are excellent examples of a widely adopted communication technology coupled with a severe threat. It's always better to get ahead of the game and be armed with technologies/solutions.

SPIT

In the messaging world, spam has become an enormous problem, with some reckonings calculating that as much as 90% of email traffic is spam. An email server can become overwhelmed with spam messages, slowing down production as users deal with unnecessary messages, and draining valuable bandwidth by clogging the network with unneeded traffic. Spam can also take an even more dangerous turn, when the spam message contains a virus, some spyware, or other type of malware. It may also try to trick recipients into going to a rogue Web site, where their identities will be stolen.

Although the security industry has stepped up to the plate with innovative anti-spam technologies, such as SmartFilter® and TrustedSource™ reputation-based technologies by Secure Computing, spammers continue to branch out and create new ways to continue with business as usual. One way is to branch out into other protocols. Already, SPIM (Spam over Instant Messaging) has started to cause problems. Now, SPIT (Spam over Internet Telephony) is expected to be the next big problem in the spam world, as spammers target growing VoIP deployments for delivery of “junk” phone calls. It would even be possible for SPIT calls to be generated the same way as SPAM messages, through networks of hijacked botnet computers.

Although SPIT is not yet a major problem, it very likely will be. And unlike many other VoIP security issues, which can be addressed with the very same technology as is used to secure standard data and messaging networks, SPIT requires special attention. Standard anti-spam technology and content filters used to protect email would not work with SPIT, because a spam phone call is not text-based. Although speech recognition may offer some relief, there are no such applications at present designed specifically to defer SPIT attacks. One of the few ways currently available to block spam voice calls is reputation-based technology, as delivered through TrustedSource by Secure Computing.

Vishing

In the email world, phishing is still a very successful scam, despite widespread education and security precautions. In a phishing email scam, a spam email disguises itself to look like a trusted source, and tricks the recipient into clicking on a rogue URL, also disguised as a trusted source, and then entering personal information, which is then collected and used for identity theft. One of the most common phishes is an attack that disguises itself as the online payment system PayPal, in an attempt to trick people to reveal their PayPal passwords. And despite the fact that almost everybody now knows not to trust an email asking for PayPal login information, it still succeeds, because people see PayPal as a trusted source. The hijacked PayPal logo lulls them into a sense of false security.

The same thing can occur over VoIP connections. Spam VoIP calls, sent out in bulk, could send recorded messages that appear to be from a trusted source, directing recipients to log into a disguised Web site, or to call back to a toll-free number, and reveal personal information.

Eavesdropping

On a standard circuit-switched telephone network, an attacker could certainly eavesdrop on phone calls, given the right equipment, and physical access to the wires, and it does happen. But eavesdropping is much easier on a VoIP network, because no physical access is necessary. If the data packets are captured (and if they are not encrypted), they can be reassembled by an attacker, and then the conversation can be replayed. This could easily be done with a man-in-the-middle attack, in which the packets would be redirected through the attacker’s system on the way to the proper destination.

Spoofing

Spoofing a VoIP phone system would be one way an attacker could potentially abuse the system to derive illicit profit. A VoIP spoof could trick a call recipient into believing that a caller was from a trusted company, and therefore reveal confidential information that could be used for identity theft. Spoofing revolves around tricking the caller ID function. Doing so is very difficult on a traditional PSTN network, but on VoIP, it is much easier. There are already in existence several caller ID-spoofing services where, for a small fee, you can select a bogus number to appear on your call recipients’ caller ID.

Solutions Available

Although the threats to VoIP do exist, those threats, just like the many other threats that exist on the Internet, can be mitigated with good technology, good policy, and education. Integrating the VoIP system into a VPN is an attractive way to add security to the VoIP phone system directly, as well as to isolate it from the rest of the network.

In many cases, security is applied by the carrier, who delivers VoIP services over a secure IPSec connection running over the Internet. Still other carriers deliver VoIP over their own proprietary MPLS (multiprotocol Label Switching) network. MPLS (also known as an IP VPN) is a common way for a service provider to create a multiservice network that carries multiple types of traffic, including voice. However, since MPLS does not secure data crossing the wire, combining MPLS with IPSec adds the ability to add encryption and authentication. What this means to the SMB user is that when they purchase a VoIP service from a carrier, there is likely to already be some level of security already there.

Besides the security provided at the carrier level, a major security/policy tool to help manage security of these converged services will be single sign-on, to ensure that every service that is being carried over VoIP is protected by the appropriate security technology, and falls under policy control.

Best Practices

Corporate cyberattacks remain prevalent, and can be devastating to a smaller company. But despite reports in the media of high-profile and costly attacks, the vast majority of them are preventable using existing technology. The first avenue of securing the VoIP network is to incorporate it into standard security best practices for data networking. A company that has a solid firewall strategy in place and sound policies, deploying an application layer firewall with unified threat management protection, access control, and content protection, will have a safe network. So too with the VoIP network. The VoIP network is not that much different than the rest of the network, and although it can fall victim to the same attacks as any Internet-facing network, it can be also protected by the same methods. Just like email and Web traffic, VoIP traffic must also be checked for viruses, spam, Trojans, spyware, and other malware.

Other best practices include changing default passwords of every component of the system, including the IP phones. Further, unnecessary applications should not be included with the VoIP system. For example, many common IP phones include a Web server, for the purpose of managing it from a PC screen. However, this strategy leaves the IP phone dangerously vulnerable.

Also, keep in mind that VoIP usually runs on a standard server with a commercial operating system, and it is therefore vulnerable to operating system flaws and hacks. It must be patched regularly, to make sure all the security updates are applied on a timely basis.

Encryption should almost always be included as part of the VoIP system. Remote users may be connected to the VoIP network through an individual multifunction security appliance With unified threat management protection and a VPN gateway. Use of the VPN protects packets by using a tunneling protocol (such as IPSec, PPTP or L2TP) to create a secure and private path through the public Internet. The resulting "tunnel" is protected because data is encrypted at one end, and decrypted at the receiving end.

Strategy of Isolation

If the first step is standard data networking best practices, the second step is embarking on a strategy of isolation. This is of course, a standard best practice, and is the foundation of Sidewinder® security appliance by Secure Computing. First of all, if it is not necessary to connect the VoIP network to the public Internet, then do not do it. However, this advice is only practical for those who wish to roll out a smaller, closed system, which would not be able to connect to other phones outside of the internal network. The bulk of VoIP installations however, seek to take advantage of broader connectivity, and will leverage the Internet for global communication capabilities.

An example of isolation is commonly seen in the corporate Internet server, which may be isolated from the rest of the network to protect it against attacks that may come in from the outside. Voice traffic too, should be deployed on a separate VLAN from other data traffic. This helps serve the security function in two ways; it prevents an attacker from coming in through the VoIP VLAN segment and getting to the rest of the network; and it also helps to preserve quality of service by protecting the VoIP VLAN from any potential denial of service attacks that may be launched against the data network.

SnapGear Solutions

A secure gateway is the foundation of a strongly protected VoIP system. Protecting your VoIP server with the SnapGear® security appliance from Secure Computing will limit access to approved users, keep attackers on the outside, and protect the network inside.

Complete with QoS controls and a SIP proxy, SnapGear is a powerful appliance that provides an ideal remote worker VoIP solution. In addition, SnapGear's L7 classifier allows VoIP packets to be prioritized over any other data being pushed through the appliance. This feature enables your VoIP calls to be as clear and crisp as any ordinary PSTN call. Designed for remote office VoIP connectivity, SnapGear offers full VoIP server functionality, and functions as an integrated Unified Threat Management (UTM) appliance. The only security appliance you will need for your company, SnapGear with TrustedSource is a versatile, all-in-one SMB multifunction appliance that can meet every small- and medium-sized business need. It can be deployed as a firewall, as a VPN gateway, a UTM security appliance, or as a complete network-in-a-box Internet appliance, with all of the wide area networking tools you need, including VoIP capability.

SnapGear brings high-quality VoIP to the SMB market at an affordable price. The most recent enhanced version of SnapGear, lends itself to VoIP in several ways. Most notably, it includes Quality of Service enhancements to allow specific types of data, such as VoIP conversations, to be assigned priority. Another VoIP-related benefit is SnapGear's VPN offloading feature, which enhances the existing VPN performance capabilities. This feature is important for those who wish to configure their VoIP systems on a VPN for added security and isolation. The VPN offloading feature makes it possible to increase the number of VPN tunnels, allowing you to connect multiple branch offices with both data and VoIP connectivity. Other performance increases in SnapGear now increase the amount of content that can pass through the appliance, and the connection-tracking snapshots give administrators the ability to identify which machines are connecting to which specific locations.

Unified Threat Management

SnapGear, as a UTM appliance, includes several tools for content and data protection, to make sure your network is free from viruses, spam, spyware, and other malicious content. This is particularly relevant to your VoIP installation, because many of the same threats that target the data network will also target VoIP.

TrustedSource

TrustedSource by Secure Computing gives SMBs with VoIP installations the ability to leverage global intelligence and behavior-based reputation scores for all IPs, domains, URLs, and email messages, in real time. Acting as the cornerstone of your VoIP security platform, TrustedSource is the front line for defense, dropping connections from malicious sources at the gateway, reducing unwanted traffic, and minimizing attacks on the network. Traditionally, such a technology would only be available to larger enterprise-level customers, but Secure Computing has made this leading edge technology available to smaller businesses through its SnapGear product offering. SnapGear is the only network security solution providing such a sophisticated system to the small business owner.

The concept of identifying spam based on the identity of the sender began years ago with traditional blacklists. These are typically lists of IP addresses of computers that have been identified as spam senders. Historically, there has been much controversy around blacklists because of the subjectivity of getting placed on the list and the difficulty of being removed. Whitelists have been developed to complement blacklists, which maintain lists of legitimate senders. A problem with whitelists and blacklists is they left a sizable set of senders in the middle of the spectrum that were not classified. This is because there was not enough credible information or feedback to make a "yes" or "no" decision about the sender. To address this problem, reputation systems for email became a topic of interest in the industry around the end of 2003 and beginning of 2004.

Reputation systems focus on monitoring sender activity, analyzing the behavior, and determining a reputation for the sender. The reputation can be thought of as a sort of credit score. In the credit scoring system, every individual is given a credit score based on some analysis of one's past financial behavior. In a similar nature, reputation systems aim to assign every computer on the Internet an email reputation. Typically, a reputation system uses the IP address of a computer as the identity and a reputation is built for that identity. There are many characteristics that can be analyzed to build the reputation including the mail volume, sending rate, complaint rate, received messages and even the time emails are being sent (2000 outbound emails at 3:00 AM could imply a bad source). These characteristics are analyzed to determine patterns that are consistent with legitimate senders, illegitimate senders and those in between.

In a similar manner, a reputation system can be built for VoIP to identify good callers from bad ones. Identity marks the difference between a VoIP application and others. Compared to e-mail systems, where the senders can be closely associated with IPs, in VoIP, the corresponding identities could be IP addresses or phone numbers. In addition, the characteristics used to analyze behavior patterns could be different too. Despite the subtle difference, reputation systems seem promising in answering security concerns for VoIP. By identifying sources that are not trustworthy, TrustedSource technology could potentially alleviate 80+ percent of all bad email, or even unwanted VoIP calls alleviating hardware, software and human resources.