Secure Business Telephony
With VoIP

A Technical White Paper

This paper describes secure business telephony and the issues that separate it from other voice applications, discusses implementation concerns and provides some guidelines for implementers of secure business telephony products and services.

By James P. Cavanagh
Global Telecom and Security Consultant
jpc@consultant-registry.com

July 2002

www.
consultant-
registry
.com

The Consultant Registry
Global Telecommunications & Security Consulting and Training Since 1994

This technical white paper was originally submitted on 24-June-2002 by **James P. Cavanagh** in satisfaction of the **SANS GIAC Security Essentials (GSEC) Practical Requirements - Challenge** Version 1.4 (Amended April 8, 2002), Option 1 - **Research Topics in Information Security.** Topic Approved 11 June 2002.

About The Consultant Registry

The Consultant Registry is a loose constellation of some of the top telecom and security consultants in the industry. Each have their own consulting practices, but come together on larger, or more complex, projects. In this way each of our members maintain their autonomy, but our clients still benefit from our strength in numbers.

Many of us have been involved in various aspects of infrastructure and network security for many years. Some of us have helped private industry, the military/law enforcement or both. This free security white paper is our way of sharing the essence of our expertise in the security, anti-hacking and counter-terrorism areas with as many businesses as we possibly can, as cost effectively as possible.

The Consultant Registry also provides training classes, workshops, publications and consulting in the areas of telecommunications, and infrastructure and network security. Please visit our website, **www.consultant-registry.com** - for more details on the products and services we offer and, for current information on security as well as a variety of other areas.

For additional information about this or other products or services of The Consultant Registry, please contact us:

The Consultant Registry
4405 Northside Parkway
Suite 2120
Atlanta, Georgia 30327
+1.404.760.0667
info@consultant-registry.com

Table of Contents

Table of Figures

Table of Tables

jcavanagh@consultant-registry.com / www.consultant-registry.com

Blank Page

jcavanagh@consultant-registry.com / www.consultant-registry.com

Secure Business Telephony with VoIP

By James P. Cavanagh

Abstract

This paper describes secure business telephony and the issues that separate it from other voice applications, discusses implementation concerns and provides some guidelines for implementers of secure business telephony products and services.

The Importance of Business VoIP Security

Voice over IP was first demonstrated in 1964 as a part of early Internet multimedia experiments. Due to the low bandwidth available on the early 56K NSFNet, and the expense and complexity of the hardware, VoIP was deemed "not ready for prime time". VoIP was resurrected in 1994 as a PC-to-PC application by individuals who would later found VocalTec (www.vocaltec.com).

VocalTec's VoIP client, and similar software offered by others, provided substantial cost savings by bypassing traditional phone carriers and using the Internet to carry voice calls. VocalTec's PC freeware allowed calls to be made for no additional charge beyond the cost of the Internet Service Provider (ISP) connection. As an example, in 1994 a call placed from Atlanta, Georgia, USA to St. Petersburg, Russia via Internet cost an additional fee of 0¢ per minute. A direct dialed call, at that same time, cost in excess of $1.25 per minute, depending upon the time of day and day of the week. "Free Voice" was born.

"Free Voice" was compelling for thousands of Internet users globally as it added a new, enticing dimension to Internet communications and allowed them to save hundreds of dollars on long distance telephony. By the late 1990s competition from VoIP had driven down the prices charged for traditional telephony calls between virtually all country pairs to the point that VoIP had no appreciable cost benefit. Voice over IP also had legendary connectivity difficulties and highly variable quality from call to call and service provider to service provider.

The net effect is that by the late 1990s VoIP had been labeled as "not suitable" for business. It was business, however, that was expected to provide the substantial sums of money to fuel growth of the IP networks - and voice is a critical application, especially in terms of the 'coming network convergence' of voice, data, and video. Voice must be included in the formula if the economies of scale businesses hope to achieve from the convergence are to materialize.

This brings us to the importance of security for business VoIP. Traditional telephony is not inherently secure. Business is emphasizing secure transmissions of all types of information, including voice, free from fear of eavesdropping or modification. To retrofit the massive global telephony infrastructure with voice security countermeasures would be cost prohibitive. There is also a global shift from the older circuit networks to IP-based networks for the next generation of telephony networks coupled with a focus on security. This positions secure telephony as one "killer app" for IP now and in the future.

Telephony's Three Waves

Telephony has been divided historically into three waves[1]. The First Wave, from telephony's inception in the late 1800s until 1964, was the analog era, during which transmission of voice was done in analog waves. The Second Wave, from 1964 to 1994, was the digital circuit era, during which analog voice waves were encoded as 64Kbps constant bit rate streams for transmission as digital bits. The Third Wave, from 1994 to the present - and for the foreseeable future - is the digital packet era, during which analog voice waves are encoded as digital samples, manipulated in a variety of ways, and transmitted in IP packets, Frame Relay Frames, ATM cells or other non-contiguous digital transmission units.

Ideally, the Third Wave includes transmission of voice, data and video content over a common backbone network. It is in the context of the emerging IP-based backbone that secure business VoIP arises as a critical, and differentiable, application.

Telephony, Voice and Sound

It is common for any transmission of sound over the Internet to be grouped into a single category, but this is not so. There are several different categories, depending upon the sound type and how it is handled by the application. The following table provides some of the points of differentiation.

Type	Application(s)	Buffering	Delay Sensitivity	Discard Sensitivity
Non-Real Time	Real Audio, Real Video, Movies On Demand, Just-In-Time Training, Archived Webcasts, etc	Yes - Large	Low	Medium
Near Real Time	Distance learning, "live" event broadcasts, uni-directional conferencing	Yes - Medium	Medium	Medium
Low QoS Real Time	"Cheap" VoIP Calling Cards, Low-cost VoIP Services	Yes	Low-to-Medium	Medium
High QoS Real Time	Bi-directional High Grade Telephony, Business Telephony	Minimal	High	High

Table 1 - Internet "Sound" Applications

The first three categories are of no particular interest to us in our discussion of business quality VoIP, but their presence explains what the "other" categories are, aside from business telephony. The last category, "High QoS Real Time", is the type of service needed to provider business grade telephony.

High QoS real time sound is characterized as having a high "Quality of Service". While it is desirable to transport voice, data and video across a converged multimedia backbone, "high QoS" voice is very often carried over an IP backbone that has been optimized for, and carries only, voice traffic. These specialized backbones are engineered for the shorter packet sizes of voice. The smaller voice transmission units do not compete with the normally long data packets. Benefits are not only shorter delays, but more consistency, as well as contributing to less delay variation.

Due to the specialized nature of these voice only networks the cost-per-minute and price-per-minute are usually higher than the prior types of sound transport and, therefore, normally have costs much closer to traditional telephony.

The amount of buffering, that is to say the time the digitized voice samples stay in temporary holding areas on their way from source to destination, must be minimized. There are two reasons for buffering. The first, inside the network, is to avoid discarding of information as it is shuffled onto and off of the shared transmission facilities and intermediate switching systems. The second, at the network edge prior to delivery to the destination, is to give the appearance of a smooth flow of bits by delivering them at a constant rate, rather than the somewhat choppy rate at which they invariable arrive due to issues such as network congestion. The bad news about buffering is that it adds delay to the end-to-end transmission and can accumulate to unacceptably high levels. The good news is that buffering can also be the 'magic trick' of Internet multimedia which allows the constant bit rate playback which gives both audio and video the appearance of circuit quality and isolates the actual user from the variations in packet network performance.

Finally, high quality business telephony is very sensitive to both delay/delay variation and loss of digital voice samples. Both of these must be minimized to within a range consistent with traditional digitized voice. All of these factors affect the cost and quality of sound transport for business telephony. There are other factors, as well. Any attempt to provide secure transmission for business VoIP must take all these factors into account.

Encoding, Compression/Suppression, Bandwidth, and Echo

There are a number of different encoding methods that can be used to digitize voice for transmission across VoIP. They range from constant bit rate methods used in traditional digital telephony, such as Pulse Code Modulation (PCM) and Adaptive Differential Pulse Code Modulation (ADPCM) to advanced encoding techniques such as CS-ACELP G.729 and G.723.1.

In addition to different ways of encoding analog voice in a digital format digital compression and/or suppression techniques can also be applied. Compression techniques use clever mathematical relationships to represent the same information in fewer bits while suppression techniques actually make intelligent decisions about what not to send from source to destination. Suppression allows certain information that can be inferred from the current connection context to not be sent, thereby saving valuable bandwidth on the shared transmission media. The absence of arriving voice samples can, for instance, infer the presence of silence in those interim gaps: the silence does not need to be sent, as it can be inserted at the destination using background noise generation.

Each of the encoding, compression and suppression methods offer a trade-off for the system architect between the monetary cost of the associated chips plus possible licensing fees, delay cost, amount of bandwidth utilized and the overall system complexity.

A quick review of the issues provides an important check list for the system designer and an important starting point for design trade-offs for any VoIP product for selecting encoding, suppression and compression methodologies:

- ✓ Encoding - which technique provides the best combination of performance, cost and complexity?
- ✓ Compression - should it be used and, if yes, which techniques?
- ✓ Suppression - should it be used and, if yes, which techniques?
- ✓ Monetary cost - impacts marketability of the product: the lower the cost the more profit and the easier to discount while maintaining margin?
- ✓ Licensing fees - must be paid on several of the more widely accepted new standards.
- ✓ Standards - should standards be followed or proprietary approaches be taken? Adhering slavishly to standards is expensive but allows interoperability between manufacturers - desirable for the purchaser. Proprietary approaches often introduce innovation sooner and lower initial costs though make commoditization in the marketplace difficult - often good for the manufacturer, never good for the purchaser.
- ✓ Delay Cost- impacts performance and quality and obviously must be minimized.
- ✓ Bandwidth used - becoming less important in terrestrial systems and unlicensed wireless systems, but it is still a critical issue in licensed wireless systems where the cost per bit for transmission is still extremely high.
- ✓ Echo Cancellation - should the additional cost of echo cancellation be included in the product or service or provided some other way?
- ✓ Overall System Complexity - has a dramatic impact on the reliability of a component and interoperability with other elements in a complete system.

In making these design decisions the following table, Table 2, will provide some guidance regarding possible delay in the end-to-end system once installed.

Delay Source	Fixed Sensitivity	Variable Delay
Coder Delay G.729 (5 ms Look Ahead)	5 ms	
Coder Delay G.729 (10 ms per frame)	20 ms	
(Packetization Delay included in Coder Delay)	-	
Queuing Delay 64 kbps Trunk		6 ms
Serialization Delay 64 kbps Trunk	3 ms	
Propagation Delay (Private Lines)	32 ms	
Network Delay (For Example IP Network)		
Dejitter Buffer		2-200 ms
Total - Assuming 50 ms Jitter Buffer	**110 ms**	

Table 2 - End-to-End Delay Budget Example[2]

Each element in the end-to-end connection contributes a specific amount of delay. That delay is either fixed or variable. Table 2 shows a sample end-to-end delay budget for a G.729 connection with a 64Kbps trunk, as one example.

Our guideline for "good" voice quality must take into account many different factors, but in terms of delay we will follow the ITU-T G.114 recommendation which states a target of 150ms one-way end-to-end delay. If the end-to-end connection works as shown in Table 2 we have already used 110 ms of our 150 ms delay budget, leaving only 40 ms for any security related delay, such as encryption, key exchange, etc, which will be discussed more at a later time. We will also make allowances for delays during call setup, such as key exchange and possible assured routing over a secure path, and delays that occur during the call itself, delays such as encryption delay or subsequent key exchanges.

In addition to encoding, compression and suppression there are other design decisions that have an impact on delay (also referred to as latency) and bandwidth consumption. For example, the number of voice samples put into each transmission frame has a big impact on overall quality and performance.

G.729 Samples Per Frame	IP/RTP/UDP Header	Bandwidth Consumed	Latency*
Default (two samples per frame)	40 bytes	24,000 bps	25 ms
Satellite (four samples per frame)	40 bytes	16,000 bps	45 ms
Low Latency (on sample per frame)	40 bytes	40,000 bps	15 ms

*compression and packetization delay only

Table 3 - Frame Per Packet Variations for G.729[3]

As shown in Table 3 the more voice samples per transmission unit (frame) the better the bandwidth efficiency. This is because the samples are small, at 10 bytes per 10 ms of speech, and the header bytes are used more efficiently. However, because of the increased delay due to the larger number of samples to be compressed and packetized, as well as delay waiting for the speech to be generated, the latency increases.

There is another trade-off, as well, which is not shown in this table. It relates to the impact of loss. If the end-to-end connection traverses a network that has a relatively high packet loss, such as a heavily loaded IP backbone shared with data, the larger number of samples per frame is not quite as beneficial as it appears at first. In a network with near zero loss, more samples per packet makes sense. However, in a network environment with higher loss, if there are more samples per packet, more voice content will be lost if a packet is lost. In the high loss environment the number of voice samples per packet should be minimized, if quality is to be maintained, even at the higher bandwidth usage.

It could be argued that higher bandwidth usage will aggravate the problem and cause higher losses and, while this is true, the higher losses will be more in the aggregate and will not have an appreciable impact on a single connection. This argument, therefore, is an issue debated by the company providing the backbone network because it relates more to the service levels for all users and the ability of the backbone provider to deliver on the promises of any Service Level Agreements (SLAs) they may have in place. This is still, therefore, an important issue for secure business voice, but more of a backbone than access issue.

Before we continue and consider adding encryption to our business VoIP connection, let's quickly review what we have covered so far:

1. Telephony has had three "waves". We are moving into the Third Wave: digital packet telephony.
2. There are several "sound" applications on the Internet. Our application is business telephony, which is a high QoS real time transmission with minimal buffering, high delay sensitivity and high discard sensitivity.
3. The choice of voice encoding technique and suppression and/or compression utilized has a dramatic effect on costs, delay and discarding. We must minimize discard and delay for our premium business VoIP service and allow development and delay budget for security functions, which will be discussed in the next section.

Now, armed with our basic understanding of high quality VoIP that will meet the needs of business, we will overlay the needed parts to fulfill our security mission and build this "killer app".

Encryption Algorithm, Delay and Cost

There are many different encryption algorithms available in the marketplace today. VoIP encryption is usually accomplished with a block cipher, as opposed to a stream cipher, so that each packet containing voice samples can be treated as a single element, as opposed to a part of a stream. This is crucial in most packet implementations that traverse the "best effort" IP protocol. If subsequent samples/packets rely upon prior samples/packets for decryption and samples/packets are lost or reordered, which is far more likely in IP-based networks than in the older circuit-based networks, the results would be chaotic. Chained block ciphers, therefore, are less often recommended in this environment.

At this point it is necessary to remind the reader that our topic is secure VoIP for business, which renders many of the methods developed for military use impractical for our consideration here due to the added delays, cost or complexity of the system. In actual commercial products we find many encryption algorithms. This is just a very small sampling:

Algorithm	Key Length	Product	Web Site
3DES	168 bit	VSU-10000	www.avaya.com
	168 bit	IP Axess	www.ipaxess.com
Advanced Encryption Standard (AES)	256 bit	SecuriPhone	www.securiphone.info
Blowfish	128 bit	VoxCRYPT	www.voxcrypt.com
GOST	256 bit	SecuriPhone	www.securiphone.info

Table 4 - Commercially Used VoIP Encryption Algorithms

There are also other algorithms, such as TEA[4], that, for reasons of speed of processing and low CPU usage, might also be suitable for use with business-grade VoIP, but are not covered here due to space considerations.

Other, newer, cryptographic algorithms may hold promise for the low delay characteristics needed for business class VoIP. Table 5, based upon the algorithms which made it to round 2 of the selection process for the Advanced Encryption Standard, shows delay characteristics from tests run by the United States National Security Agency.

Algorithm	Thru-put (Mbps)	Block Encrypt (ns)	Block Decrypt (ns)	Key Setup (Encrypt)	Key Setup (Decrypt)
MARS	-	-	-	-	-
RC6	1192-2171	1179-2146	1179-2146	-	-
RIJNDAEL	371-5163	247-493	247-493	-	246-344
SERPENT	202-8030	510-733	510-733	7-20	212-672
TWOFISH	38-1445	1593-3342	1593-3342	-	-

Table 5 - Encryption/Decryption Delay from NIST AES Selection[5]

As we can see in Table 5, none of the algorithms add an appreciable encryption or decryption delay. The table entries are in nanoseconds, which are inconsequential in terms of voice delay, but the actual dollar cost of implementing these algorithms may be prohibitive for VoIP applications at this time. They certainly are candidates, however, for more expensive or specialized systems that will certainly be utilized for military and high visibility private individuals.

Telephony Variations and Secure VoIP

Having laid a general framework for business VoIP telephony we will now consider the many practical implementation issues associated with business grade VoIP.

PC-to-PC

The PC-to-PC model was the first one to be developed, largely because the personal computer platform is an open, general purpose platform that can easily be programmed to perform a variety of functions.

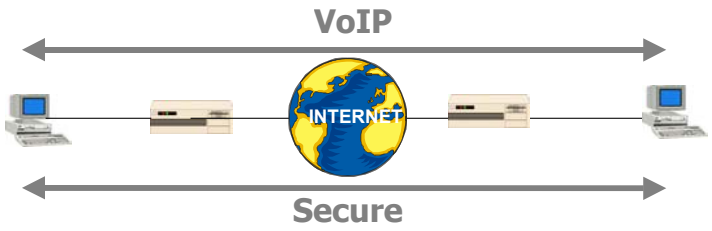

Figure 1 - PC-to-PC VoIP Model

Secure VoIP is easiest to implement between two Personal Computers due to the wide range of implementation options possible on that platform. One such example is VoxCRYPT. "VoxCRYPT is a Windows application that allows you to talk (actually send voice, not typed characters) over a TCP/IP network. If your network connection isn't fast enough to support real-time voice data, various forms of compression may allow you, assuming your computer is fast enough, to converse nonetheless. To enable secure communications, encryption with 128-bits Blowfish is provided. Your communication records and cryptographic keys are stored on a 128-bits 3DES secure VoxCARD smartcard."[6]

The PC-to-PC model, however, is the least well suited to the needs of the business telephony user. This model has very problematic call set-up, varies widely in performance and quality when voice traffic leaves the controlled environment of the corporate VPN and traverses the Internet, and, maybe most importantly, requires the use of a PC to initiate and terminate a call.

Another issue is that both the calling party and the called party must have PCs with the same secure VoIP software initiated. This is not a suitable model for business VoIP.

PC-to-Phone

The PC-to-Phone model was an obvious extension of the PC-to-PC model. The PC-to-Phone model utilizes a VoIP/PSTN gateway in the local calling area of the destination telephone to allow a call to hop off of the IP packet network and onto the local Public Switched Telephone Network (PSTN).

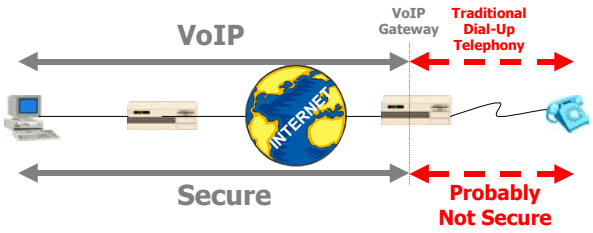

Figure 2 - PC-to-Phone VoIP Model

This is more suitable than the PC-to-PC model for business telephony as it alleviates many of the call set-up issues, because this approach allows the PC to 'dial' a normal, properly formatted telephone number. There is still the issue, however, of the caller having to have a PC to initiate calls.

A secure telephony issue with this model is the fact that we can do secure telephony across the Internet or VPN, but are not assured secure communications across the PSTN part of the connection. In the 'last mile', an area where traditional eavesdropping could be performed, we must have security or our efforts at a secure end-to-end connection are for naught.

Phone-to-PC

For reasons of interworking problems between public telephone switching and the Internet the phone-to-PC application has only been pursued on a very limited basis and does not offer promise for business VoIP.

Phone-to-Phone

The Phone-to-Phone model is the one that works best for business telephony because calls are made the same way as they always have been - from a traditional telephone to another traditional telephone. This model allows the standard PSTN dialing plan to be used to access a local PSTN/IP gateway where all standard call control signaling is converted into IP packets for transmission across the IP network using IP addresses and traditional routing. The destination X.121-formatted phone number is translated to a destination IP address in the originating gateway. At the destination gateway the look-up and dialing of the local number is performed.

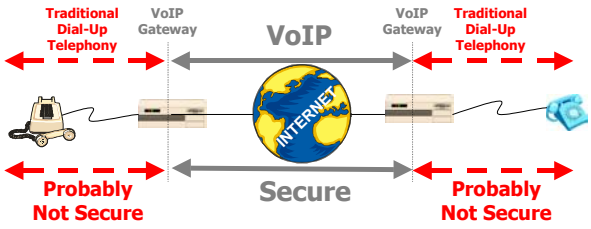

Figure 3 - Phone-to-Phone VoIP Model

Issues here involve security of the voice call from the phone to the IP network on both the originating and terminating ends. This can be highly problematic and is an Achilles heel of this type of telephony. The access issues can be substantial and are addressed in the next section.

Access Issues

Access issues are the issues of getting to and from the IP network. Many voice encryption systems encrypt from one handset to another, while many VoIP based security systems ignore how a user accesses the network and begins security inside the confines of the IP network.

Tandem Coding occurs when voice goes from a system requiring one type of coding to a system requiring another type of coding. For instance, a call is originated on a PC using G.723.1 voice encoding and the call subsequently hits a corporate Public Branch eXchange (PBX) from whence it is routed onto a Public Switched Telephone Network (PSTN). In this case the encoding must be changed from the G.723.1 to G.711 Pulse Code Modulation (PCM). This process is called tandem coding and every time this occurs delay is introduced and voice quality declines. Some tandem coding pairs are worse than others, but all pair combinations introduce delay and quality degradation.

Mobile Wireless represents the most important access technologies for the business person on the move. Many mobile wireless access systems interconnect across their terrestrial portions using traditional PCM type networks, while others use IP-based networks. In any case, it is still possible to have tandem coding and encryption/decryption issues between the wireless and terrestrial portions of the network as well as when traversing the interface between two different backbone networks.

Wireless Local Loop/Unlicensed Wireless Fixed wireless systems, such as Wireless Local Loops (WLL) and unlicensed wireless systems such as 802.11x are also being used increasingly for VoIP. The good news, overall, is that these type of systems often terminate calls to PCs that are capable of running their own local encryption and decryption, assuming the user invokes it. An alarming number of wireless LANs, for instance, do not even enable the rudimentary Wireline Equivalent Privacy (WEP). Even though it is easily cracked by hackers, WEP at least provides an additional level of protection against the casual snoop.

It is also possible to solve these types of problems by running secure tunnels from a secure client on one end of the connection to the other. In this case, the information going across the wireless portion is encrypted and secure by default.

Satellite has its own set of issues. In addition to the wireless issues previously addressed, satellite may have additional delay issues. There are multiple types of satellite systems. While it is a gross overgeneralization, in general the GEO, or geostationary satellites tend to support traditional telephony and have the greatest delay and highest price telephony services. The LEO or Low Earth Orbit, satellites tend to provide IP-based telephony services and have minimal delay and lower service price. There tend to be tandem coding issues with GEOs and not as often with the LEOs. Another flavor, the Mid Earth Orbit (MEO) satellite is not used for bi-directional transmission, only for broadcast transmissions.

Having considered the many forms of wireless access, we will know briefly review the many traditional and emerging forms of terrestrial access.

Cable Modem based "...VoIP services are subject to a spate of potential security issues that PacketCable is attempting to address. ... CableLabs outlines a litany of potential threats in its PacketCable security specification, including theft-of-service, snooping and protocol manipulation. Among the theft-of-service threats, PacketCable lists subscription fraud, non-payment for services and a potential proliferation of [Media Terminal Adapter] MTA clones, which could register themselves under a fraudulent account. Another possible threat is denial of service, whereby someone tries to inject bogus packets into the system to bring the system down.

PacketCable also addresses 'bearer channel information disclosure' attacks such as simple snooping, a privacy assault in which voice packets sent in the clear could be compromised. Protocol manipulation, yet another potential threat, could allow a hacker to discover bearer channel encryption keys.

PacketCable has adopted a conservative approach to these threats by layering on security specs designed to protect signaling and messaging channels and to essentially make VoIP as hackproof as possible. DOCSIS already provides encryption between the [Cable Modem Termination Service] CMTS and the MTA, but on top of that, PacketCable mandates that the bearer channel is encrypted again and that the speech path is encrypted as well."[7]

Digital Subscriber Line (DSL) most often connects PCs to a private, VPN or public IP network. Even though the physical connection is very different the security issues are fundamentally the same as addressed in the section above on cable modems.

Frame Relay and ATM, like DSL, typically connect either PC clients and/or routers, gateways, and other systems to IP-based networks. For this reason the issues are pretty much the same as cable modems, as well.

T1/E1, T3/E3, SONET/SDH are historically used for channelized traditional 64K PCM connections, in which case there will be tandem coding issues as well as encryption/decryption issues. Increasingly, however, these historically Time Division Multiplexing (TDM) connections are being used in a non-channelized format which gives them similar characteristics and issues for the other packet transport access connections listed above.

Other Technical Issues

There are a myriad other issues which are well beyond the scope of this white paper, but the following represent some of the more pertinent technical issues which need to be addressed for a successful implementation of secure business VoIP. While each one could be a full white paper of their own they are addressed briefly here to be sure they are considered carefully by anyone implementing secure business VoIP. Additional references and resources may be found at the end of this document.

Interoperability

One key area of concern in security in general, and in secure business VoIP in particular, is that of interoperability. If secure calls will only be placed intra-company, this is less of an issue as all secure telephony devices can be sole-sourced from the same manufacturer and there will be no interoperability issues. This is what many areas of the military does to 'solve' the problem. Problems arise, however, when they wish to conduct secure communications with the military leaders of other countries with incompatible systems.

Another solution is to perform VoIP across interoperable IPSec-compliant systems treating VoIP traffic as you would any other traffic, or possibly prioritizing VoIP traffic to a higher level. In this case, as early experimentation has shown, it is possible to achieve an acceptable level of voice quality for regular use. However, as certain limits are pushed, such as physical distance between callers or number of tandem hops grow, the quality often degrades to levels below those which are acceptable for high quality business voice traffic.

Suitability of IPSec for Secure VoIP

IP-based networks using IPSec security, especially for intra-company communications over VPNs are being found to be quite suitable for secure VoIP calls. It is not cost effective, however, to build an IPSec-secured infrastructure simply for the purpose of securing VoIP calls. The costs are too high, the structure too complex and the protection not matched well enough to the content.

"IPSec allows IP packets to be encrypted, a mode known as Encapsulated Security Payload (ESP). It also assures the integrity of the message by creating a MAC of the IPSec packets, known as Authentication Header (AH). The eavesdropping threat ... can be countered using ESP encryption, while packet spoofing, replay and message integrity can all be countered, to a large extent, by AH authentication and, to a lesser extent, by ESP encryption. Thus, the use of VPN/IPSec technology can successfully protect against many ... network threats."[8]

For that mixed voice, data and possibly video environment IPSec can be quite suitable and developers are already releasing toolkits for IPSec that can quite readily be adopted in the secure VoIP arena. Most of the toolkits are sufficiently sophisticated to allow fine tuning of those parameters with the biggest impact on the quality of the business-grade secure connections. Toolkits are discussed in greater length later in this document.

Key Management and Distribution

If the framework of IPSec is utilized for secure VoIP key management and distribution is included under the umbrella of IPSec in the Internet Key Exchange (IKE) and Internet Security Association Key Management Protocols (ISAKMP). Otherwise, key management and distribution will be an issue. Most implementations will likely rely on some variant of Diffie-Hellman public key exchange, from which there are several viable candidates to choose.

Development Tool Kits

Several different organizations provide security developer's toolkits. Developer's tool kits provide the underlying protocol and interface modules and allow the Independent Software Vendor (ISV) or private companies to develop applications using the specific protocols and interfaces without having to develop original code. The benefits of developer's tool kits are numerous, but the main benefits are a dramatic shortening of the application development, testing and deployment cycle and an a near guarantee of interoperability with other products and systems developed using the same tool kit.

Among the most widely utilized security tool kits that can be applied to business-grade VoIP are IPSec and cryptography tool kits from a variety of vendors. Among the leading vendors are Entrust (www.entrust.com), RSA Security (www.rsasecurity.com) and SSH Communications Security (www.ssh.com).

Test Suites

Test suites are also an important part of the VoIP security picture. The use of standardized test suites helps to assure interoperability and standards compliance and are useful in the product development, product selection and implementation phases. Be cautious, however, because two different products may both pass compliance testing independently but they may not, necessarily, interoperate. After initial testing against the test suite, products that are to be interconnected must be tested with each other prior to final acceptance.

In the case of business class VoIP there are two areas that are crucial to test: the first is the quality of the voice itself, and the second is the security and standards compliance of the underlying security system.

Voice Quality

Voice quality over the secure system is vital for acceptance by business people and the ultimate "killer app" designation we are striving for. There are two basic approaches to voice quality measurement. The oldest and most widely accepted is MOS and the newer, and more controversial, are PQSM/PAMS/PESQ, which are described below.

Mean Opinion Score (MOS) is the approach used for the last several decades and involves a panel of "judges" listening to certain voice and sound sequences and rating them on a scale of 0 to 5, with 5 being the best. It is widely believed that Pulse Code Modulation (PCM) is the 5 rating benchmark, which is actually not true. In most MOS tests PCM is usually the best, but only ranks in the 4.0 to 4.1 range. It is possible for newer methods to better PCM's quality performance.

Within the MOS test category, it is also possible to use the CMOS, or comparative MOS. Comparative MOS does not use a ranking scale, per se, but rather is based on the present sound sample being better or worse than the prior one. MOS is an expensive process, but it is the best test possible.

Compression Method	Bit Rate (Kbps)	Sample Size (ms)	MOS Score
G.711 PCM	64	0.125	4.1
G.726 ADPCM	32	0.125	3.85
G.728 Low Delay Code Excited Linear Predictive (LC-CELP)	15	0.625	3.61
G.729 Conjugate Structural Algebraic Code Excited Liner Predictive (CS-ACELP)	8	10	3.92
G.729a CS-ACELP	8	10	3.7
G.723.1 MP-MLQ	6.3	30	3.9
G.723.1 ACELP	5.3	30	3.65

Table 6 - ITU-T Codec MOS Scoring[9]

Table 6, above, shows Mean Opinion Scores for various ITU-T voice compression methods. The MOS will provide a selection guideline for anticipated voice quality from any given encoding method.

Perceptual Speech Quality Measurement (PSQM), Perceptual Analysis Measurement System (PAMS) and Perceptual Evaluation of Speech Quality (PESQ) are all computer models that purport to lower the overall cost of voice quality testing by using a computer instead of a human listener to evaluate overall quality. PSQM is the earliest attempt in this area and leaves a great deal of room for improvement. There are many ways in which voice digitization and transmission systems can fool the fallible human ear into a sense of higher quality, but PQSM can't be 'fooled' so easily and, therefore, PQSM provides ratings that vary substantially from the human ratings, rendering its results useless.

"PAMS is a major innovation in speech quality assessment. It was the first model offering reliable assessment over a wide range of networks, including VoIP, in 1998. It goes further than ITU-T recommendation P.861 (PSQM/MNB), which is for testing only codecs. PAMS measures one-way quality. It is designed for use with intrusive tests: a signal is injected into the system under test, and the degraded output is compared with the input (reference) signal."[10]

"PESQ measures listening quality of speech over a wide range of networks and codecs in accordance with the ITU-T standard P.862. Psytechnics have also made extensions to allow PESQ to be used for Head and Torso Simulation (HATS) and wideband telephony. PESQ measures one-way quality. It is designed for use with intrusive tests: a signal is injected into the system under test, and the degraded output is compared with the input (reference) signal."[11]

Many points should be considered prior to settling on a testing strategy, but MOS should always be used, where and when possible.

Protocol Compliance and Interoperability

There are many different organizations globally that provide protocol compliance and interoperability testing. There are none better, or who have been doing the job longer than the International Computer Security Association (ICSA) Labs (www.icsalabs.com), now a division of TrueSecure (www.truesecure.com).

"The goal for ICSA Labs' Certification Program is to improve commercial computer trust and security. Recognizing that perfect computer security is unattainable, the computer security industry pursues technological improvements and practical risk reductions. ICSA Labs' Certification Program provides assurance that products reduce security risks consistent with a set of publicly vetted and industry accepted criteria. ICSA Labs' Certification process is dynamic. Successive versions of the Certification Criteria include greater levels of risk reduction yet are attainable with available technology and an average knowledge for applying the technology.

The ICSA Labs' IPSec Product Certification Program has the objective to make available to the user community an ever-increasing selection of multi-vendor IPSec products that are interoperable and that provide the security services of authentication, data integrity, confidentiality, and non-repudiation."[12]

Both voice quality testing and protocol/interoperability testing must be a part of any comprehensive secure business quality voice initiative.

Practical Considerations of Securing Business Telephony

Having addressed some of the important technical issues of secure business telephony, we will now take a look at some of the practical issues.

PSTN and VoIP Voice Security

Invariably at the present time, and for the foreseeable future, virtually all business telephone calls using VoIP will, at some point, traverse the Public Switched Telephone Network and be subject to traditional eavesdropping. There are several devices which operate over any telephony system and are, in fact, transport independent. For organization's requiring the highest grades of security, and willing to give up some convenience in return, there are always devices such as *The Scrambler* [13], the *Voice Scrambler TS-400*[14] or similar devices.

VPN vs. Internet Business VoIP

Many businesses operate their own large private IP networks or procure pre-packaged IP networks called Virtual Private Networks (VPNs) from carriers or service providers. The VPN is not actually a private network, but rather a portion of a public network, often using the global Internet. The user organization has the perception of privacy due to the security mechanisms put in place to 'wall them off' from other users. They get the best of both worlds: privacy due to security, but with the economies of scale of the public Internet.

VoIP security issues in this area are also important to consider. Most of the foregoing considerations apply to the VPN but "[t]here are other reasons companies don't use VoIP over a VPN network today. Full-scale VPNs don't make sense for every company due to security concerns and the difficulty of convergence integration. Also, today VPN offers secure services using encryption schemes. While encryption can be used with VoIP, encryption and decryption would add latency and degrade QoS — probably to the point where business customers would find it unacceptable.

To use VoIP over VPN, encryption would mostly likely need to be turned off for calls that end up outside the VPN — again, probably unacceptable to most businesses. Access to the corporate LAN by way of unauthorized VoIP access is simply too big a risk for most businesses to take."[15]

Cost

Cost must be kept as low as possible so that the final price to the end-user is kept to a minimum. Experience in the marketplace has shown that while security features are highly desirable the bottom line likelihood of most customers to pay a premium for security is very low. What has been demonstrated, though, time and again, is that if two competing products or services have the same - possibly discounted - price and one has security features and the other does not that the security features are a positive product differentiator. It is also desirable to have a version of the product without the security features or where a security feature may be permanently disabled.

Ease of Use

Ease of use is one of the most important features of any security product, feature, service or system. In fact, user over-riding of security mechanisms or total disregard for their use go far beyond the common stories of people writing their complex user ids and passwords on Post-It™ notes and posting them near their screens. Security systems that place even a small operational hurdle in front of a busy business person are likely to be totally ignored, or if possible, completely bypassed for systems that are easier to use.

Legal and Regulatory Issues

Legal and regulatory issues are also important considerations for secure business voice. The legality and status of both VoIP and encryption is not certain in all countries.

VoIP

In many countries around the world the use of VoIP or any other systems to bypass the government owned and operated Postal Telephone and Telegraph (PTT) Authority is illegal and can result in heavy fines and possibly arrest and detention. Be sure to check local regulations when arriving in country. In many cases the restrictions only govern ISPs, but often regulate private networks or VPNs, as well.

Cryptography

Once it has been verified that VoIP is legal in the country, it is also mandatory to determine if the overlaying cryptography needed to make the business VoIP secure is also legal, and if legal, what other restrictions may apply in terms of encryption algorithms, key lengths, etc. Even though this information should be verified in country upon arrival, a good Internet source is the Global Internet Liberty Campaign[16]. They maintain reasonably current cryptographic legal, regulatory and policy information and links for many countries around the world as well as other entities, including the European Union.

Other Business Voice Security Issues

Other business voice security issues that must be considered include:

- ✓ Security of calling cards and account information
- ✓ Security of passwords and access codes for telephony and voice mail systems.
- ✓ Assuring temporary buffers, such as on hotel and conference room telephones, are cleared after use.
- ✓ Proper handling and disposal of telephony logs and bills
- ✓ Physical security of cell phones and other devices

All areas of potential vulnerability must be closed in a manner consistent with the risk, budget and potential damage caused by their exploitation.

Conclusion

Secure business telephony with VoIP might just be the 'killer app' for which the Internet marketeers are searching. Like any security discipline every facet of the technology must be viewed and reviewed to assure that all knowable exploits are blocked and all vulnerabilities are patched. And, like any security discipline, we must be ready to react quickly when new vulnerabilities are discovered and new exploits are disclosed.

Secure business telephony, like other areas of security, is a goal that is nearly achievable in the interim, but it, too, will likely remain a chess game without a checkmate.

List of References

References

Anderson, John. "Methods for Measuring Perceptual Speech Quality" (22 October, 2001)
URL: http://literature.agilent.com/litweb/pdf/5988-2352EN.pdf

Cavanagh, James P. "Internet and Internetworking Security", Copyright 1997, Auerbach/RIA Group.

CheckPoint Software's Secure Virtual Network (SVN) Architecture First to Secure IP Telephony (5 October 1999)
URL: http://www.checkpoint.com/press/1999/telephony100599.html

Delivering high performance VoIP over VPN (20 March 2002)
URL: http://www.voiceanddata.com.au/vd/feature_article/item_032002a.asp

Guevin, Laura. "Be Careful How You Call: VoIP Is Illegal In Many Countries" (31 January 2000)
URL: http://www.tmcnet.com/tmcnet/columns/laura013100.htm

Kaufman, Charlie, et al. "Network Security - Private Communication in a Public World", Copyright 1995, Prentice Hall.

Mel, H.X and Baker, Doris. "Cryptography Decrypted", Copyright 2001, Addison Wesley.

Molitor, Andrew. "Securing VoIP Networks with Specific Techniques, Comprehensive Policies and VoIP-Capable Firewalls" (No Date)
url: http://www.aravox.com/literature/aravox_specifictechniques.pdf

Pieprzyk, Josef and Tombak, Leonid. "Soviet Encryption Algorithm" (24 November 1993)
URL: http://www.rave2.com/Gost.zip

Pracht, Stefan. "Voice Quality in Converging Telephony and IP Networks" (22 October 2001)
URL: http://cp.literature.agilent.com/litweb/pdf/5980-0989E.pdf

Psytechnics. "Speech quality assessment in wireless applications" (May 2001)
URL: http://www.psytechnics.com/technical.html

Stringfellow, Brian. "Secure Voice Over IP" (15 August 2001)
URL: http://rr.sans.org/VOIP/sec_voice.php

Weiss, Eric. "Security Concerns with VoIP" (20 August 2001)
URL: http://rr.sans.org/VOIP/sec_concerns.php

Cited References

[1] Cavanagh, James P. "Three Waves of Telephony" (1 October 2001)
URL: http://www.consultant-registry.com/delivery/3wavesoftelephony.pdf

[2] Davidson, Jonathon. "Voice over IP Fundamentals", Copyright 2000, Cisco Press, Page 191.

[3] Davidson. Page 172.

[4] Wheeler, David, et. al. "TEA, a Tiny Encryption Algorithm" (November 1994)
URL: http://www.ftp.cl.cam.ac.uk/ftp/papers/djw-rmn/djw-rmn-tea.html

[5] Weeks, Bryan, et al. "Hardware Performance Simulations of Round 2 Advanced Encryption Standard Algorithms" (No Date)
URL: http://csrc.nist.gov/encryption/aes/round2/conf3/papers/37-bweeks.pdf

[6] VoxCRYPT Advanced Digital Scrambler Software (2001)
URL:http://www.voxcrypt.com/en/products/voxcrypt.html

[7] Baumgartner, Jeff. "Piecing together the VoIP puzzle", CED Magazine, (May 2001)
URL: http://www.cedmagazine.com/ced/2002/0502/id7.htm

[8] Ganley, Dr. Michael J. " Security and Performance Issues Associated with Voice and Video Over Internet Protocol (August 2001)
URL: http://www.cylink.com/library2/white/voip8-01.pdf

[9] Davidson. Page 174.

[10] Psytechnics. "PAMS: Measuring speech quality over networks...as the customers hear it" (May 2001)
URL: http://www.psytechnics.com/papers/PAMS_1.1.pdf

[11] Psytechnics. "PESQ: Measuring speech quality over networks...as the customers hear it" (May 2001)
URL: http://www.psytechnics.com/papers/PESQ_1.0.pdf

[12] ICSA LABS Program for IPSec Product Certification (6 March 2002)
URL: http://www.icsalabs.com/html/communities/ipsec/certification/index.shtml

[13] The Scrambler (Date Unknown)
URL: http://www.pimall.com/nais/e.privacy.html

[14] Voice Scrambler TS 400 (Date Unknown)
URL: http://www.eaprotection.com/eguipment/telefax.htm

[15] Machi, Jim. "VPN: The Enterprise VoIP Darling", (January 2002)
URL: http://www.tmcnet.com/it/0102/0102ii.htm

[16] Global Internet Liberty Campaign, "International Cryptography Page"
URL: http://www.gilc.org/crypto/

Index

Q

R

S

T

V

W

X

About The Author

James P. Cavanagh

Global Telecom & Security Consultant

James P. Cavanagh has worked closely with five of the predominant communications technologies of our time very early in their life cycles. He has been intimately involved with the engineering, sales support, marketing, design, installation and training for ATM, Frame Relay, IP, optical networking and xDSL since their early commercialization. Mr. Cavanagh has also been intimately involved in network security, disaster recovery planning and infrastructure security since the early 1980s. Jim is able to combine his experience with creativity and a long, varied career to develop exceptionally effective solutions for his consulting clients as well as having a rich background for his teaching and writing. Jim is a former member of the ATM forum.

Mr. Cavanagh's consulting practice is built around three primary areas: traditional consulting, writing and training. In the area of traditional consulting Mr. Cavanagh boasts a long list of recognizable clients in the areas of network and infrastructure security, IP, ATM, Frame Relay, DSL and optical networking as well as traditional telephony areas. The client list includes manufacturers, carriers, service providers and end-user organizations whom he has helped with everything from product specification to network procurement, design, integration, installation, engineering, marketing, business planning and tactical and strategic planning. Mr. Cavanagh's clients are quick to point out that Jim brings major projects in consistently on-time and on budget.

Jim is an internationally recognized expert on infrastructure and network security, anti-hacking, counter-cyberterrorism and business and corporate security. In the fall of 2001 he completed a very well attended five city Canadian tour as a part of the TELUS Expert Series which received good press coverage and attendance in light of the events of September 11 and is continuing his heavy involvement in consulting, writing and training in the security area. For additional security related information, please see The Consultant Registry **Focus on Security** Page.

Mr. Cavanagh is the editor of books on multimedia networking and network security as well as author of *Frame Relay Applications: Business and Technology Case Studies*. He is presently writing a book on network and infrastructure security aimed at the corporate and business market, and is starting a new website covering domestic US and International telecom regulatory and legal issues. Mr. Cavanagh is also the author of several popular computer based training (CBT) programs covering Frame Relay, emerging broadband technologies, fiber optic communications basics and advanced fiber optic network design in addition to over three dozen articles for trade publications and journals.

Mr. Cavanagh is also a frequent guest on panels at industry conferences, has been an instructor for the International Communications Association's (ICA) Summer Program at the University of Colorado at Boulder from 1992 until 1997 and is the recipient of the ICA's Citation of Merit Award for "outstanding contributions to global telecommunications". Mr. Cavanagh provides training on ATM, Frame Relay, Emerging Technologies, LAN and TCP/IP Integration, Telecom and Datacom Fundamentals and a variety of other subjects to over 2,500 telecommunications professionals each year. Mr. Cavanagh is very active with the Atlanta Telecom Professionals (ATP), an organization for telecommunications professionals in Atlanta. The Consultant Registry is a Gold Sponsor of ATP.

www.
consultant-
registry
.com

The Consultant Registry Security Skills Training Series

SECURITY SKILLS TRAINING SERIES

A comprehensive series of 3 technical training courses on security topics.

In addition to management, organizational policy, security awareness and related security consulting and training **The Consultant Registry** offers a full range of technical consulting services and training. **The Security Skills Training Series** is comprised of three courses: an introductory class, and intermediate class and an advanced class, designed to be taken as a series or independently. Additional information on these and other courses is available on the web at www.consultant-registry.com.

Infrastructure and Network Security™Theory & Practice™, 2 Day Class. *The Infrastructure and Network Security Theory and Practice*™ course is an introductory level course covering a wide range of areas related to the security of network and operational infrastructure. This is an ideal course to use as a stepping stone to other, more advanced topics, or as a general introduction for organizational security or law enforcement personnel. This course is designed for everyone from the network administrator of a small to large corporation, non-profit organization or academic institution to local, state and federal law enforcement personnel involved in network and infrastructure security, anti-hacking and counter-terrorism. It does not matter if the risks to your network or assets are competitors, industrial spys or international terrorists, this course has a rich, broad content applicable to a wide variety of security needs.

Network Security Theory & Practice™, 2 Day Class. This course is an intermediate level course. This is an overview course with a lot of breadth and is designed for the telecommunications networking professional. We refer to this one as a "smorgasbord course" because it offers a little of everything. This course will be of particular interest to individuals wishing to build a base of knowledge that will allow them to go on to our more advanced courses. A lot of emphasis is placed on encryption, hacker techniques, and overall security policy, technology and implementation. This course is ideal for the individual who has just been told by management that they must develop and implement a security program within their organization. This course includes the comprehensive "Network and Infrastructure Report Card" assessment tool as well as a comprehensive security review covering all seven layers of the OSI model.

Network Services Security™Theory & Practice™, 2 Day Class. A two day class designed for organizations providing network services and Virtual Private Networks (VPNs), such as Internet Service Providers (ISPs), Network/Backbone Service Providers (N/BSPs), carriers and large organizations managing their own intranets and private IP networks. This class has been very well received by nationally recognized IP service organizations in the US and Canada and is typically attended by network engineers, security professionals and technical managers.

To better understand how **The Consultant Registry** can help your organization contact us at 404.760.0667 or via email at info@consultant-registry.com.

The Consultant Registry

Telecommunications & Security Consulting and Training Since 1994

4405 Northside Parkway, Suite 2120 Atlanta, Georgia 30327 USA

+1.404.760.0667 - www.consultant-registry.com