Global Information Assurance Certification Paper

Secure Voice over IP
Brian Stringfellow
August 15, 2001

Introduction

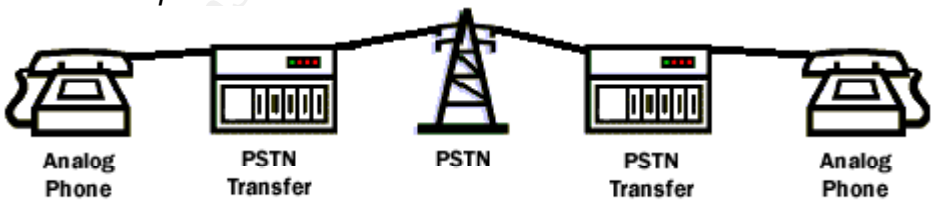
The purpose of this document is to give a general overview of Voice over IP (VoIP) and to explain the essential security issues surrounding a successful VoIP deployment. The scope includes the "big three" signaling protocols, vocoders, and the mechanisms used to secure VoIP.

A brief history

Since the invention of the telephone in the late 1800's, advances in communication have brought us great features, better quality and near-perfect reliability. However, through use of dedicated circuits, the traditional telephone system has grown to the point of diminishing returns. By virtue of its architecture, circuit-switched telephony is inefficient by today's standards. To place a call, an end-to-end circuit must first be available and is then tied up for the duration of the call. While not in use, it sits idle. For example, the capacity of a standard T-1 line is 24 lines, or simultaneous calls. Voice is sampled using Pulse Code Modulation (PCM) at 64K per channel. With an added 8k of overhead, the total (x 24) amounts to 1.544Mb. In addition, PCM does not use any type of compression. While the voice quality is very good, the use of bandwidth is inefficient.

Diagram A illustrates the path of a call using traditional telephony equipment. While very simplistic, the intent is to demonstrate that a 64k circuit is use end to end.

A. Traditional Telephone Connection



On the other hand, packet-switched telephony, which shares bandwidth on data circuits, can handle as much as twelve times the traffic using standard and/or proprietary compression algorithms. Vocoders employing compression are now is use that replace PCM. Conventional wisdom would dictate, "you get what you pay for", however, with voice compression that is not always the case. Test labs continuously prove that more data does not necessarily equate to better voice quality. You are urged to test many vocoders before adopting a standard for your organization. In the digital wireless arena for example, compression is

used across-the-board and generally goes unnoticed. In fact, PCS carriers use call clarity as a selling point.

Following is a partial list of standard vocoders.

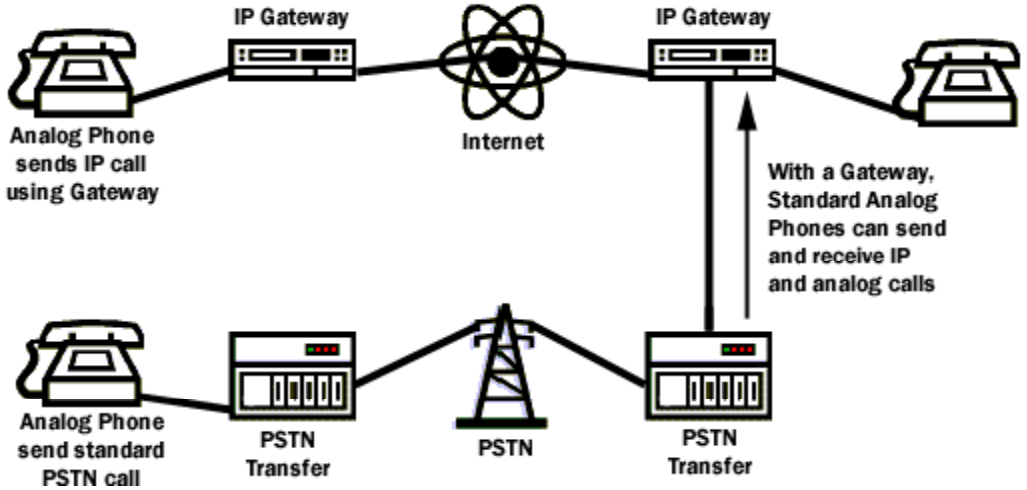
G.711 (PCM)	64K
G.726	16, 32K
GSM	12.2K
G.729(a)	8K
G.723.1	5.3, 6.3K

In addition to these standard vocoders, some VoIP manufacturers have dedicated R&D resources to writing proprietary vocoders that are widely used and accepted as toll-quality.

Diagram B illustrates how an IP telephony system integrates with the Public Switched Telephone Network (PSTN). This is just one of many VoIP scenarios in which gateways are deployed to connect to Class-5 switches at a central office (CO). This is how it became possible to place a call from a PC running an H.323 client (such as Net2Phone) to a regular telephone number. This diagram could easily be altered to have PCs as endpoints, rather than analog telephones. Typically, at the low end, a VoIP gateway will have a T1 or E1 interface on the line side to send channelized voice traffic to and from a traditional class-5 switch. At the upper end, many gateways support multiple Optical Carrier (OC) connections handling thousands of voice channels.

On the network side, connections to the Internet are generally Ethernet interfaces anywhere from 10Base-T to Gigabit in speed that connect to high-speed routers for wide-area transport. The main point being demonstrated below is that voice compression takes place, bandwidth is shared, and multiple paths can be taken through the Internet increasing efficiency and reliability.

Voice over IP System



In the early days of packet telephony, carriers and enterprises maintained

security by controlling traffic end to end. Time Division Multiplexing (TDM) and Voice over Frame Relay (VoFR) networks were private and, therefore, less vulnerable to intrusion. As Voice over IP was introduced, quality and interoperability issues restricted its use to private networks as well. But, as quality issues improved, namely latency, carriers and enterprises began to run traffic across the Internet and privacy was maintained through obscurity. Albeit hardly secure, proprietary vocoders and protocols gave VoIP carriers a somewhat false sense of security as other issues, such as availability, were overlooked. The assumption being that to capture and replay a conversation successfully would be very difficult. Chances of having the motive, opportunity, skill set, hardware and software to eavesdrop or disrupt communication were still so remote as to keep developers from addressing the security issue head-on and innate vulnerabilities persisted.

Threats

Traditionally, threats to the circuit-switched telephone system include such things as wire tapping, unwanted (disturbing) calls, account fraud, call masquerading, and denial of service. On a packet-switched network, many of these issues remain while others are overcome. The equivalent of wire-tapping can be achieved through packet sniffing anywhere in the path of voice traffic. To counter this, encryption is used to prevent decoding of voice packet payload.

Recent advances have been made to prevent disturbing calls via the PSTN. With “call screening” and “anonymous call rejection” this issue being addressed on the PSTN and newer VoIP networks as well.

The issue of call masquerading is left up to the caller to authenticate their counterpart in a conversation. Users will not tolerate being required to enter a PIN before answering the phone at their desk or home. While it would be possible on either type of phone network, I have not been able to find any implementations of it.

Denial of service (DoS) is a constant threat to any type of network system. Since DoS attacks can originate anywhere and by anyone, they are often the most difficult to counter. In the following section I will address how each VoIP protocol type counters this threat.

Open Communication

With the growing popularity of VoIP throughout the 90’s, developers began to work toward open standards in call signaling (MGCP/Megaco, H.323, SIP) and vocoders types (G.729(a), GSM, G.723) in hopes of achieving interoperability. Clearly, this would be a necessity if packet-switched telephony is to someday replace traditional circuit-switched telephony.

H.323 – Intelligence everywhere

An H.323 solution is comprised of intelligent endpoints known as Terminals, Gateways, Gatekeepers, and Multipoint Conference Units (MCUs). What began as a LAN-based technology has evolved and adopted features that address security. H.235 is the security mechanism that H.323 uses to protect the audio stream as well as the Call Setup (A.931) and Call Control (H.245). H.235 attempts to provide security features such as Authentication, Integrity, Privacy and some non-repudiation support in H.323 communications. However, lawful interception, which is required by most governments, has degraded much of the protection offered by H.235.

A secure Call Setup is achieved using TCP port 1300. Once established, Call Control is initiated so that encryption and media channel information can be negotiated. Most often, H.323 utilizes RTP/RTCP (real-time transport protocol) as its transport protocol, which rides over UDP where encryption is performed within the RTP packet, by third party hardware, or at the network layer (IPSEC).

H.323 can use either symmetric encryption-based authentication or subscription-based authentication. Subscription-based authentication can be certificate-based (asymmetric) or symmetric, which is password-based (with or without hashing).

MGCP – Intelligent network with dumb endpoints

Media Gateway Control Protocol was defined by the Media Gateway Control (MEGACO) working group in RFC 2705. Under RFC 3015, the same working group updated MGCP, which then became known as “MEGACO”.

MGCP Call Control is secured using IPsec with an Encapsulating Security Payload (ESP) header, assuming the underlying network and operating systems support it. Otherwise, an interim Authentication Header (AH) solution may be used. When using IPv6, only ESP may be used. The AH header allows for data origin authentication, connectionless integrity and optional anti-replay protection of messages passed between the Media Gateway (MG) and the MGC (Controller), but does not provide protection against eavesdropping or replay attacks. However, in IPsec, the Integrity Check Value (ICV) is calculated over the entire IP packet including the IP header, which prevents spoofing of the IP addresses.

Another issue is known as “uncontrolled barge-in” where voice packets can be directed to a gateway on the appropriate UDP port. Unless protection is in place, the audio will be heard on the line side. To counter this, the gateway will only accept data from a predetermined IP address and UDP port. The down side is that it adds processing overhead and can be spoofed. To counter spoofing, the MGC obtains “remote session description” from the initiating

gateway and passes it to the destination gateway, thus increasing call setup time. However, by using a secret key to encrypt and authenticate packets, call setup time will not be increased.

SIP – Intelligent endpoints with dumb network

Session Initiation Protocol (SIP) development began in 1996 and was approved by the IETF as a standard in 1998. Similar to HTTP, it uses a "request-response" model and can establish communication between two clients without the necessity of an intermediary device. Using simple text commands, a session is initiated and either accepted or rejected. In most cases it is routed by a proxy or redirect server. The SIP protocol itself seems to rely on third party security for the most part. The only consideration to security threats is in its support of PGP authentication and encryption. An Internet Draft now addresses this issue.

"The SIP security framework", an IETF draft by Michael Thomas, addresses two classes of threats. First, the framework addresses threats that originate from basic transport considerations (i.e., vulnerabilities of transporting SIP in the clear over UDP and TCP). Next, the framework addresses threats which originate at the SIP application layer, and where the participating entities in a transaction may not be trustworthy. SIP relies on transport layer security mechanisms such as TLS or IPSEC to provide the required security for the whole message. The framework does not specify a means of cryptographically protecting MIME messages, but instead provides a framework for use of other crypto-systems, such as PGP. The general format of a SIP message using this framework is a main IP message header, followed by any number of MIME attachments. The actual contents of the attachments, beyond the required headers to implement the crypto-system, are normal SIP headers, which are intended to be protected. Unlike message/sip attachments, the contents of a sip-secure attachment should be viewed as a continuation of the headers in the main header section of the SIP message.

Constraints

There is always a "give and take" in any design and security solutions are no exception. Users' expectations and secure protocol designers play tug-of-war and a compromise must be made. Quality of service is the number one problem VoIP network designers face today. Latency is a paramount issue as users will not accept long call setup times, delay in conversation, or choppy voice quality (jitter). As stated earlier, a secure voice network employs encryption end-to-end thus introducing more latency. On a network with a fair amount already, this may be unacceptable. The acceptable limit has been set at about 200 milliseconds so many Internet links are not ready to handle real-time traffic such as voice or video. Participants in a conversation will begin to talk over each other as latency increases above 200ms. With the addition of

video, the problem is exacerbated making live teleconferencing impossible.

When passing traffic between carriers and across public networks, there is often a need for network address translation (NAT) and firewall transversal. When network layer information is applied at the upper layers, the firewall must be aware of this to perform the translation or "fixup" properly.

Conclusion

The promise of next generation services and potential cost savings that VoIP will bring makes the offering very viable for enterprises and carriers worldwide. Forecasts predict "worldwide revenue from next-generation services will grow from $74 million in 2000 to nearly $40 billion in 2006. In the US, the most advanced market for next-generation services, revenue will grow from US$28 million in 2000 to US$15 billion in 2006, by which time application services will account for 58% of all next-generation service revenues in the US." (Delaney) To ensure this level of growth, care must be taken to provide a secure infrastructure. From design to deployment, security is essential in providing quality of service to the users and profitability to manufacturers and carriers. While there are literally billions invested in today's infrastructure, IP telephony will continue to make strides in replacing this infrastructure as particular attention is paid to making it secure.

Sources:

Alachi, Joanna. "Standards Snapshot: The State Of The Big 3 in VoIP Signaling Protocols" 27 November 2000. URL: http://www.commweb.com/article/COM20001127S0008 (17 Sep. 2001).

Marjalaakso, Mika. "Security Requirements and Constraints of VoIP" URL: http://www.hut.fi/~mmarjala/voip (17 Sep. 2001).

Liu, Jing. "The Security Architecture of H.323" URL: http://www.hut.fi/~yanli/Jing/home.html (17 Sep. 2001).

RFC 3015 "Megaco Protocol Version 1.0" November 2000. URL: http://www.ietf.org/rfc/rfc3015.txt?number=3015 (17 Sep. 2001).

Thomas, Michael. "SIP Security Framework" 12 July 2001. URL: http://search.ietf.org/internet-drafts/draft-thomas-sip-sec-framework-00.txt (17 Sep. 2001).

Delaney, John and Hall, Peter. "Next-Generation Services: Impacts on the Industry and Markets." June 2000. URL: http://www.tdap.co.uk/uk/archive/internet/int(ovum_0006).html (17 Sep. 2001).

“How VoIP is Implemented.” URL:
http://www.e-telcorp.com/voip/implemented.htm (17 Sep. 2001).

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event