Global Information Assurance Certification Paper

Secure VoIP: Why, how and for what cost?

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Tommi Simula
Location: SANS London 2004

Paper Abstract: The implementation of data encryption on VoIP networks, technical challenges and weaknesses of different methods.

Table of Contents

Abstract 1
Introduction 1
ITU-T H.323 1
Session Initiation Protocol (SIP) 2
MEGACO/H.248 3
Current VoIP shortcomings 4
Goals and Requirements 5
Authentication 5
Confidentiality 6
Integrity 6
The Candidates 6
Secure RTP 6
IPSec and Virtual Private Networking 7
Conclusion 8
Designing a secure system 9
Securing an existing system 10
Footnotes 11
References 12

Abstract

This paper discusses the implementation of data encryption on VoIP networks. The main objective is to identify the main technical challenges and weaknesses of different methods and technologies, and the suitability of these methods in different scenarios with different standards and protocols. The main aspect to be covered is data confidentiality, but other considerations, such as integrity and authentication, will also be inspected.

Introduction

Public Switched Telephone Networks (PSTN), aka our traditional analog telephone systems are inherently insecure. Secure transmissions of all information are becoming more and more important to all businesses and communities, and retrofitting the existing infrastructure with adequate countermeasures would be cost prohibitive. The movement from the old circuit-based networks towards packet-based IP-networks for transmitting voice information is aiming to patch these issues, but majority of the current implementations are lacking or immature in many areas. When implementing any new technology, the aim should be to improve all areas, not just remain on the same level. IP telephony makes it possible to not only improve the security, but also improve quality and introduce new functionality. The new generation of telephony networks needs to be implemented from the ground up with a focus on security, but improving also other areas to achieve wide-spread acceptance.

Voice over IP (VoIP) is a technology for transmitting and managing voice information over Internet Protocol (IP) networks. Instead of a traditional analog telephone, the phone calls can be placed with for example a Windows PC, an IP-telephone or a PDA device. The VoIP network is connected to the PSTN with a gateway. Let's take a quick look at the major VoIP standards by the standards bodies governing multimedia delivery over packet-based networks, International Telecommunications Union (ITU), Internet Engineering Task Force (IETF) and Media Gateway Control Working Group (MGCP WG):

ITU-T H.323

The H series recommendations are ITU standards that define audiovisual and multimedia systems. H.323 is group of ITU-T recommendations for packet-based multimedia conferencing, which defines real-time audio, video, and data over packet-switched networks. It addresses problems related to packet delay and packet loss, which are common issues on packet-switched networks.

A H.323 system consists of a PSTN/IP gateway, a Multipoint Control Unit (MCU) used for conferencing, a gatekeeper for authentication and terminal devices. The key protocols used in H.323 are Real-time Transport Protocol (RTP), Real-time Transport Control Protocol (RTCP), H.225 RAS (Registration, Admission, Status), H.225 Call Signaling, H.245 Control Signaling, and various video and audio codecs. RTP is a common factor over practically all VoIP standards for the delivery of audio and video data. It runs over UDP and is optimized for real-time transmissions utilizing the multiplexing and error-checking features of UDP. RTCP is used to control and synchronize streaming audio and video. It provides feedback information to the source that can be used to adapt the flow to changing network conditions. The terminals and the gatekeepers manage call registrations, admissions and terminations with H.225 RAS, which also uses UDP as a transport. The terminals communicate between themselves using H.225 over TCP and H.245. The connections between two terminals are opened using H.225 signaling, the control messages for flow control, opening and closing of channels, capacity management and general commands and identifiers are sent using H.245.

H.235 defines security and privacy for H.323 and other H.245 based terminals. It can be used with both point-to-point and multipoint conferences. H.235 defines three methods for authentication, password-based with symmetric encryption, password-based with hashing and certificate-based. By default, HMAC-SHA1-96 hashing is used for integrity. Supported 'external' authentication methods are via IPSec and TLS. The H.235 data encryption is implemented on the RTP layer, supporting algorithms ranging from DES to Triple DES and AES. H.323 also creates additional issues with firewalls, due to its dynamically allocated ports for audio, video and data channels. Applying all the supported techniques, authentication, integrity checking and encryption, protects against a number of common attacks, such as denial-of-service, man-in-the-middle, replay attacks, connection hijacking, spoofing and eavesdropping. H.235 does not, however, provide non-repudiation. While existing on paper, the H.235 extensions are very rarely implemented.

A recent test conducted by the NISCC discovered several vulnerabilities in the H.323 protocol stack with several vendor implementations [1].

Session Initiation Protocol (SIP)

Where H.323 is a more traditional approach, largely specified by the telecommunications companies, SIP is an IETF standard protocol that provides simple application layer signaling for setting up, maintaining, and terminating multimedia sessions such as voice calls, videoconferences, and even instant messaging sessions. SIP performs many of the functions of the H.323, but is better scalable, higher-performance, and more efficient. It is independent of the packet layer, can run on both UDP and TCP, and supports out-of-band signaling.

With OOB signaling the call and control signaling takes place over IP, but the actual voice data is transmitted over PSTN. SIP can also be used with other protocols, but the IETF SIP architecture includes the following:

- RSVP for reserving network resources
- RTP for transporting real-time data and providing QOS feedback
- RTSP for controlling delivery of streaming media
- SAP for advertising multimedia sessions via multicast
- SDP for describing multimedia sessions.

The main components in a SIP-based system are a User Agent Client (UAC) for call initiation, a Proxy Server and a Redirect Server or a User Agent Server. SIP supports two forms of encryption, end-to-end where the SIP payload is encrypted, and hop-by-hop where the SIP requests and responses are encrypted to prevent finding out the source, destination or the route of the packets. Hop-by-hop is easier to implement in practice since only the service providers need to set up a PKI infrastructure, but as a disadvantage it causes transitive trusts to be created. All SIP authentication mechanisms are challenge-response based, with basic, digest and PGP-signed alternatives. SIP itself provides very limited means for encryption, only PGP encryption of certain headers is supported. To be useful, this requires a PKI infrastructure to be established. SIP packets carry the session IP addresses and TCP ports in the body, which causes problems with NAT and firewall traversal, since the body has to be unencrypted for the device to be able to do the translation.

SIP hasn't been without its problems either, in February 2003 several vulnerabilities in the vendor implementations were reported by CERT, which could lead to unauthorized privileged access, cause denial-of-service attacks or unstable system behavior [2].

MEGACO/H.248

MEGACO, a new version of Media Gateway Control Protocol (MGCP) by Media Gateway Control Working Group and the similar standard by ITU, H.248 will be combined and published as a single document. The original MGCP version 1.0 specification can be found at http://www.ietf.org/rfc/rfc2705.txt. The security of the standard is based on IPSec and IKE, either AH or ESP is expected to be used with control connections, but not with media connections. Therefore, all security related issues with MEGACO/H.248 are basically issues or limitations of IPSec.

Current VoIP shortcomings

With today's VoIP implementations, by default, all data is sent in clear text. RTP streams can be recorded or relayed. Very little vendor support exists for encryption and alternative solutions are often complex and offer poor performance. Some VoIP systems for MS Windows platform require the user to have local administrator rights, and to add the VoIP servers in the Internet Explorer trusted sites. Remote management of systems is usually done via telnet or http, using weak passwords and plain text authentication. Sessions can be hijacked and denial-of-service attacks are trivial to execute. With access to the network and widely available tools such as tcpdump and vomit [3], a user can record network traffic and convert Cisco IP phone conversations into standard wave audio files. One approach to prevent eavesdropping, i.e. listening to conversations without consent, is to use a separate dedicated network for VoIP traffic. However, a dedicated network is costly, and requires additional administration and monitoring, therefore virtually all current implementations share the office LAN to transmit voice traffic. In this case the best solution is to use a switched network, and to separate voice traffic on its own VLAN. While this may deter some abusers, tools such as dsniff [4] can be used to circumvent these protections and capture traffic over separate segments of a switched network. The issues with VLANs are discussed in detail in Steve A. Rouiller's paper "Virtual LAN Security: weaknesses and countermeasures". [5]

Even using a dedicated network doesn't ensure security. A voice packet carried over IP is data, with all its vulnerabilities, and should be handled with the same care as any mission-critical data. Encrypting the data is an effective way to prevent, or at least impede eavesdropping attempts, but there are several other aspects to be dealt with. Voice communications are a real-time service by nature so long response times when having a conversation are unacceptable. While delays of over 1000ms caused by network congestion may be unnoticeable with regular file transfers, a latency of 50ms in a VoIP conversation may be the difference between high and unusable quality. Encryption/decryption is a strenuous task, and requires large amounts of processing power. The process of encrypting the whole packet, where the header and the payload are used to form a new encrypted packet with a new header, causes additional overhead and larger bandwidth requirements. Furthermore, local legal requirements may demand that government officials have the possibility to wire-tap phone calls under certain situations.

Implementing security measures to a VoIP system impedes the already sensitive real-time nature of the service. Fast processing speeds are required from the devices to achieve transparent latency-free encryption. Things can be improved by using compressed audio codecs, such as G.723/G.729 for H.323, to lessen the bandwidth requirements. Using compression degrades audio quality, but used in moderation can dramatically improve performance with only a small to unnoticeable sacrifice in quality. However, according to Jim Metzler, an analyst

with Ashton Metzler and Associates in Sanibel, Florida: “Encrypted data running over [virtual private network] tunnels is difficult to compress, because the data does not conform to expected patterns.” [6].

When the VoIP network is shared with other services, which usually is the case, Quality of Service (QoS) schemes can be used to prioritize traffic based on for example the type of service fields of the IP datagrams. To be useful, the protocols and all network devices need to support the used QoS standard. This might be problematic considering all the various standards, a quick search for “qos” at the IETF website [7] turns up with no less than 247 internet drafts mentioning the word. However, correctly implemented and combined with traffic shaping, that is smoothing out the peaks and lows of data transmission, a QoS scheme can guarantee that other services won’t disrupt VoIP traffic, and the levels of jitter and latency remain acceptable. QoS can also be implemented together with different VPN tunneling methods, provided that the vendor supports it. Cisco Systems mentions in its Cisco IOS QoS features documentation the following about IPSec: “For IPSec tunnels, the command is applied on the crypto map, allowing configuration on a per-tunnel basis. QoS features on the physical interface carrying the crypto map are able to classify packets before encryption”. [8]

Goals and Requirements

There are several different possibilities for securing voice communications, each with their strengths and weaknesses. This section tries to shed some light on the different methods and techniques.

Authentication

Authentication is a process to verify someone's identity and we need to be certain the person accessing the system is who he claims he is. Usually this is done based on the IP address, which can’t be considered as a secure method. Challenge-response authentication is based on a handshake between the client and the server. The server issues a challenge, and the client must reply with a response, typically a password. There are several implementations on challenge-response, e.g. CHAP, which is used for HTTP authentication. In its basic form challenge-response provides only a very light level of security, because the handshake is transmitted in plaintext. To change this, several methods are available. A simple method is instead of the actual password to just send a cryptographic hash of it, such as MD5 or SHA. Most smart cards and other hardware access token systems are based on a challenge-response system. There is nothing to stop you from using several different methods simultaneously either, such as requiring both a certificate and a password to authenticate, but the measures taken and the tediousness of the use of the system should be in sync with the level of confidentiality required.

Confidentiality

Confidentiality means ensuring that only authorized people have access to our data. Authentication is one measure towards this goal, but it can usually be circumvented. Encryption, if implemented correctly, is a very effective tool, and is considered vital for ensuring confidentiality of sensitive data. Implementing encryption however, is not quite trivial, and the different methods have very distinct differences in their behavior. Encryption is typically implemented either on the packet/frame level (e.g. IPSec tunnel mode), application level (e.g. SSL), or by only encrypting the payload of the IP packet (e.g. IPSec transport mode). The method to be applied in a certain scenario depends on various facts, such as the level of confidentiality of the data and the security of the network. While encrypting just the data portion of the packets prevents the eavesdropping of the actual conversation, the headers will still reveal the identity of the participants. If encryption for one reason or the other is not practical or possible, and the security of the network and its components can be ensured to a degree, a switched network layout can be used as a rudimentary defense.

Integrity

The easiest way to ensure, that the message that was sent has not been tampered with or corrupted when it reaches its destination, is to use a one-way cryptographic hash. The data is run through an algorithm, which outputs an irreversible, fixed-length and unique hash. After the transfer is finished the algorithm is run again on the same data in the other end, and the two hashes are compared. If the hashes match, it can be said with a level of certainty relative to the security of the used algorithm, that the message has not been altered.

The Candidates

The issues with current VoIP implementations and specifications are known, and substitutive or complementary specifications are in development, or just waiting to be widely adopted. The security standards for H.323 and SIP based systems were already discussed earlier in this document; let's have a look at what else we can use.

Secure RTP

Standard Real-time Transport Protocol (RTP) is used for VoIP traffic. It supports DES-CBC encryption, doesn't define secure authentication and uses MD5 for deriving encryption keys. An excellent paper on RTP security by Ville Hallivuori from Helsinki University of Technology Finland can be found at http://www.iki.fi/vph/files/rtp_security.pdf.

Secure RTP (SRTP) is a suggested new profile of the RTP protocol that provides encryption, secure authentication and replay protection. SRTP supports various encryption algorithms, such as AES-CM (AES Segmented Integer Counter Mode) for data encryption and session key derivation and HMAC-SHA1 for authentication and message integrity. The default key length is 128-bit for data encryption and 112-bit for session salt keys. The default key length for authentication is 160-bit. These are the minimum/default requirements, longer key lengths and other algorithms can be used. SRTP encrypts only the payload of the IP packets, which has both positive and negative effects. The IP header of the packets remains unchanged, so the implementation won't affect QoS, and the headers can be compressed for more efficient bandwidth usage. On the other hand, this also leaves the headers open for reading any sensitive information contained within, and tampering the headers, which might cause problems when routing traffic through insecure networks, such as the internet. The SRTP specification allows for weak or NULL authentication to be used, but strong authentication should always be employed where possible. Even with the payload encrypted, insecure authentication makes denial of service and replay attacks possible. Automatic key management and unique master keys for each SSRC should be employed to avoid two-time pads and SSRC collisions, where a reused encryption keystream within a session may cause a serious security compromise. [9]

IPSec and Virtual Private Networking

Let's finally take a look at a current technology that can be used to secure basically any existing implementation. IP Security (RFC 2401) was created to provide a security architecture for IPv6, but the slow migration from IPv4 has made it already fairly popular. IPSec is a set of protocols to ensure, as the name suggests, security on the IP layer. IPSec protocol suite provides means for packet-level security and key exchange. Encapsulating Security Payload (ESP) is the most common one used for encryption, and at this point only one protocol, Internet Key Exchange (IKE) exists for key management.

There are two basic modes of IPSec, transport mode and tunnel mode. The tunnel mode is used with VPNs, and transport mode to encrypt the data segment of IP packets. VPN tunnels not only strengthen confidentiality by symmetric encryption algorithms, they also provide secure authentication and integrity checking. A VPN encapsulates all of the traffic inside an encrypted tunnel, which reaches end-to-end, making it ideal for uncontrolled environments, such as the internet. The data is in encrypted form only while in transit, and is invisible to the end user and the application. Supported symmetric block cipher algorithms include 3DES, Blowfish, IDEA and RC5. While being arguably the most secure method, it also has significant drawbacks. Encryption with a long key length is a time consuming process and requires a lot of processing power to be achieved in real-time. Encrypted data also requires more bandwidth, for example an IPSec in tunnel mode with 3DES encryption may cause up to 850ms latencies and even

up to 90kbps additional overhead per call [10]. Another issue is remote connections through a firewall. While most current firewalls support VPN pass-through, and can filter out all packets except those with VPN headers such as ESP, at the same time we also lose the ability to filter and log the traffic inside the tunnel. Tackling these issues has been one of the largest constraints of wide-spread adoption of VPN tunneled voice traffic.

IPSec defines a protocol called Authentication Header (AH) for secure authentication. AH uses a shared key to create an Integrity Check Value (ICV) with e.g. HMAC-MD5 or HMAC-SHA1 algorithms. Anti-replay sequence numbering is enabled by default. AH however does not provide data encryption, and therefore is not widely used, however, combined with an efficient data encryption scheme such as ESP can provide a viable authentication method.

The IPSec key negotiation protocol IKE uses Diffie-Hellman key exchange with either public or pre-shared keys or digital certificates. The mechanism is considered secure against eavesdropping, but vulnerable to man-in-the-middle attacks, unless using signing by digital certificates. The use of certificates is recommended, but requires a public key infrastructure.

Conclusion

The main drawbacks with encryption are performance and quality related. When implementing any encryption scheme, not to even mention a 'D-I-Y' solution on top of an existing product, the network performance should be thoroughly stress-tested before rollout. Minor sacrifices in voice quality should be tolerable, when the alternative could be finding confidential business-critical conversations publicly circulated over the internet. The theoretical implications of encrypting and compressing audio data are well-known, but currently the amount of publicly available real world test material about the performance and quality issues are limited. For organizations concerned about the performance of different products, test reports can be purchased from certain research and consulting companies, such as The Tolly Group [13]. There are also several test suites available and testing services are provided by a plethora of vendors.

Based on the findings, the biggest obstacle is the immaturity of the standards and products. Few vendors provide out-of-the-box secure products that are easy to implement. On a corporate level, building a VoIP infrastructure requires big investments and resources, and if the product is found to not support secure authentication and encryption mechanisms, changing to a different scheme may well mean a complete overhaul of the system. The decision of which technology to implement depends on a variety of issues, let's take a look at a few of the key ones.

Designing a secure system

When designing a new VoIP environment, careful planning and weighing of the alternatives should be done. The product vendor should ideally be able to purvey a solution that natively supports the required technologies. The checklist for the knowledgeable VoIP systems shopper should include at least the following items:

- Support for encrypting signaling and media traffic
- Secure authentication methods with integrity checking and non-repudiation
- Compatibility with all signaling protocols
- Dynamic per-call firewall control
- Dynamic per-call bandwidth control
- Failover and redundancy options
- Remote management using HTTPS/SSH
- Active systems health monitoring
- Call usage reporting and call tracking capabilities.

Secure RTP standard has just been finalized in March 2004, and products based on this can be expected in the near future. H.235 provides means to create a secure H.323 infrastructure, but is seldom implemented. Even if the product supports some sort of proprietary security marchitecture [11], it's vital to make sure the functions are viable and adequate. The system is as strong as its weakest link, therefore the encryption method has to support a well-known and tested algorithm with a sufficient key length, and the implementation has to be functional yet watertight. The Committee of National Security Systems (CNSS) rates the AES algorithm as acceptable for encrypting top secret data on their AES policy fact sheet, CNSS Policy No. 15, Fact Sheet No. 1: "The design and strength of all key lengths of the AES algorithm (i.e., 128, 192 and 256) are sufficient to protect classified information up to the SECRET level. TOP SECRET information will require use of either the 192 or 256 key lengths." [12]. Of course, encryption using AES with even a 128-bit key length means that nothing short of a supercomputer can break it in any reasonable amount of time, and this hardly is required in every scenario. A 56-bit DES encryption is considered unacceptably weak by today's standards for confidential material, but is still dramatically better than no encryption at all. Using lighter encryption schemes where maximum security isn't required and available bandwidth or processing power on the terminal devices is limited, is acceptable and even advisable.

Encryption should take place on the transport level, and also secure the header information, if the nodes of the network can not be trusted. The headers can identify the participants of the conversation, and in some cases even contain confidential data, such as credit card information. Still, remote access methods, such as laptops and PDA devices connecting over the internet or other wide area networks bring out other issues. While using transport level security blocks out, or at least hinders severely any eavesdropping and replay attacks, the price is the loss of traffic control on the perimeter. Unless we can be absolutely certain

the accessing device can be trusted, it might even be sensible to favor packet level encryption on remote devices over using encrypted VPN tunnels to prevent network breaches, and sustain the ability to audit and filter incoming connections at the firewall. What it all boils down to is priorities, whether the confidentiality of the VoIP system considered a bigger risk than a breach in network security. Risk assessments should be carried out and measures taken based on the results. However, this is true with all VPN connections from outside f the network, and only really a concern here if the connections are solely built for VoIP traffic. If VPN connections are in use for other purposes already, utilizing these is self-evident. Inside trusted networks such as LANs, where all nodes can be secured and monitored actively, a hop-by-hop mechanism is a valid option.

The authentication should optimally be based on digital certificates using PKI, and provide hashing to provide integrity checking and non-repudiation. These should be preferred over conventional password-based methods like challenge-response.

Securing an existing system

If the organization already has implemented a VoIP system by some product vendor, the primary approach should naturally be to implement security enforcements supported natively by the product. When this is not possible, IPSec and other low level tunneling schemes can be implemented with virtually any software application, but requires firmware support when using dedicated IP phones. IPSec provides reasonably robust protection, combining symmetric block cipher algorithms with secure authentication. If the organization already has an existing public key infrastructure, the start-up costs should not be unreasonable. Application level tunneling, such as SSL, requires support from the software, and should be used for remote management purposes, and with connections with web based VoIP clients. As with any type of system, trying to secure an existing VoIP infrastructure that has not been designed from the ground up with security in mind, may prove impractical or even impossible.

As a conclusion, the risks involved with IP voice communications are very real and can cause serious damage unless measures are taken. Encrypting the data connections when transmitting over insecure networks should be considered mandatory, with encrypted VPN tunneling as the most secure option. Inside trusted networks encryption is highly recommended, and should be implemented whenever possible. Even more important than encryption, is providing a secure authentication mechanism that ensures the identity of the users. While encryption is considered optional in certain situations, with authentication and integrity checking, there is no excuse. If your organization still doesn't have a public key infrastructure, maybe this is the right time to proceed with the plans.

Footnotes

[1] “NISCC Vulnerability Advisory 006489/H323”, Jan 2004. NISCC. http://www.uniras.gov.uk/vuls/2004/006489/h323.htm (11.10.2004)

[2] Oostenbrink, L. “CERT Advisory CA-2003-06 Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP)”, Jun 2003. SURFnet CERT.
http://cert.surfnet.nl/s/2003/S-03-011.htm

[3] Provos, N. “vomit - voice over misconfigured internet telephones”.
http://vomit.xtdnet.nl/

[4] Song, D. “dsniff”.
http://www.monkey.org/~dugsong/dsniff/

[5] Rouiller, Steve A. “Virtual LAN Security: weaknesses and countermeasures”, GSEC Practical Assignment.
http://www.sans.org/rr/papers/38/1090.pdf

[6] Korzeniowski, P. “Squeezing more capacity out of WANs”, Aug 2004. FCW.com.
http://www.fcw.com/fcw/articles/2004/0830/feat-wan-08-30-04.asp

[7] “ht://Dig Search results for 'qos'”, 2004. The Internet Engineering Task Force.
http://search.ietf.org/cgi-bin/htsearch?restrict=http://www.ietf.org/internet-drafts/&words=QoS

[8] “Quality of Service for Virtual Private Networks”, 2004. Cisco Systems.
http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a0080080404.html (11.10.2004)

[9] Baugher, M. etc., page 36-41.

[10] “Document abstract“, IP Telephony: Bandwidth Effects of VPN Tunnels on VoIP Traffic - Volume 1, Issue 8, Jun 2001. The Tolly Group.
http://itresearch.forbes.com/detail/RES/993657859_159.html (11.10.2004)

[11] “The Inquirer jargon: The "seamless" union of architecture and marketing, exemplified in the long-running "chip wars" over "clock speed" and such campaigns as "Intel Inside".”, 2004. The Inquirer.
http://www.theinquirer.net/?article=8069 (11.10.2004)

[12] "CNSS Policy No. 15, Fact Sheet No. 1 - National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information", Jun 2003. CNSS Secretariat. http://www.nstissc.gov/Assets/pdf/fact%20sheet.pdf (11.10.2004)

[13] "VOIP by The Tolly Group", 2004. Accountancy Age IT Research Library. http://accountancyage.bitpipe.com/rlist/905740864_63/VOIP.html (11.10.2004)

References

"Draft revised Recommendation H.323 V5 (for Consent)", May 2003. ITU-T. http://ftp3.itu.int/av-arch/avc-site/2001-2004/0305_Gen/h323V5consented.zip

"H.235: Security and encryption for H.323 (and other H.245-based) multimedia terminals", Javvin Company Protocol Dictionary. http://www.javvin.com/protocolH235.html (11.10.2004)

"Security and encryption for H-series (H.323 and other H.245 based) multimedia terminals, Version 3", May 2003. ITU-T. http://www.javvin.com/protocol/H235v3.pdf (11.10.2004)

Percy, K., Hommer, M. "Tips from the trenches on VoIP", Jan 2003. Network Fusion. http://www.nwfusion.com/research/2003/0127voip.html

"PKI Overview", Dec 2003. Trustees of Dartmouth College. http://www.dartmouth.edu/~deploypki/overview.html

Baugher, M., McGrew, D., Naslund, M., Carrara, E., Norrman, K."RFC 3711 - The Secure Real-time Transport Protocol (SRTP)", Mar 2004. The Internet Engineering Task Force. http://www.ietf.org/rfc/rfc3711.txt

Baccala, B. "IPSec Protocol Overview", Connected: An Internet Encyclopedia. http://www.freesoft.org/CIE/Topics/141.htm (11.10.2004)

Handley, M., Schulzrinne, H., Schooler, E., Rosenberg, J. "SIP: Session Initiation Protocol", Mar 1999. http://www.ietf.org/rfc/rfc2543.txt (11.10.2004)

Marjalaakso, Mika. "Security Requirements and Constraints of VoIP". http://www.hut.fi/~mmarjala/voip (11.10.2004)

Kent, S., Atkinson, R. "RFC 2401 - Security Architecture for the Internet Protocol", Nov 1998.

http://www.ietf.org/rfc/rfc2401.txt (11.10.2004)

Kent, S., Atkinson, R. “RFC 2406 - IP Encapsulating Security Payload (ESP)”, Nov 1998.
http://www.ietf.org/rfc/rfc2406.txt (11.10.2004)

Kent, S., Atkinson, R. “RFC 2402 - IP Authentication Header (AH)”, Nov 1998.
http://www.ietf.org/rfc/rfc2402.txt (11.10.2004)

Harkins, D., Carrel, D. “RFC 2409 - The Internet Key Exchange (IKE)”, Nov 1998.
http://www.ietf.org/rfc/rfc2409.txt (11.10.2004)

Allsop, Wil. “VoIP - Vulnerability over Internet Protocol”, Mar 2004.
http://www.net-security.org/article.php?id=667 (11.10.2004)

Last Updated: July 25th, 2017

Upcoming Training

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