TECHNICAL WHITE PAPER

Avaya Media Encryption

Version: **1.02**

Date: **July 12, 2004**

CID: **105413**

Author: **Avaya Technology and Consulting**
Corporate Systems Engineering

Abstract:

The confidentiality of business telecommunications has often been taken for granted. There are three primary reasons behind this prevailing attitude. First, because of the separation of telecom and data networks, the threat of snooping or tapping into telecom lines required access to the specific physical medium used by the targeted conversation. Second, the risk associated with this potential tapping vulnerability was mitigated to an acceptable level by enterprise physical security safeguards. Third, the skill set to carry out this operation, although not advanced, required knowledge and insight into the process.

With the convergence of the telecom and data networks, the risk of snooping has dramatically increased and rendered the previous risk assessment invalid. Converged networks alter the physical to the logical. Traditional analog and digital circuit based technologies used for voice communications have been replaced with packetized voice samples. These samples are then carried within Internet Protocol packets which are capable of being routed around the world in mere milliseconds. User friendly Internet downloadable software has been created and is available which can easily decode, record and play back these samples, dramatically reducing the required skill set of the attacker.

Avaya Understands the Issues

The majority of all IP Telephony and VoIP vendors utilize the IETF's Real Time Protocol in combination with well-known codecs such as G.711 and G.729 for the transmission of the voice bearer channel over an IP network. This "commonality" can rather easily be exploited across vendor implementations to listen in on “private" voice conversations. Eavesdropping is limited in scope in the classic telephony end-point architecture of digital and analog sets. Each end-point has a dedicated “wired” connection between itself and the call processing platform. Unauthorized snooping requires physical access to this wired infrastructure. Additionally, Avaya digital sets convert voice energy into a digital format using proprietary encoding before transmission across this wire so more than a butt-set and a pair of "alligator clips" would be necessary for successful voice interception.

The requirement for physical access for snooping is in stark contrast to the openness of a packet based environment used by IP based sets. Through various well documented methods such as packet sniffing, ARP poisoning/man-in-the-middle, or port mirroring, Real Time Protocol packets can be captured, recorded, and even played back using cookie-cutter decoding tools exploiting the "open" nature of these underlying protocols. These tools are downloadable from the web or can be crafted together from publicly available source code. A common customer misconception to this tapping problem is that a "switched" data network prevents the use of such decoding tools. This is entirely just that, misconception. An excellent SANS article explaining practical sniffing in a switch network topology underscores this point and can be downloaded here: Packet Sniffing In a Switched Environment.

What Avaya offers

Avaya proactively developed a privacy solution based on the ITU H.235 (Security and encryption for H-series H.323 and other H.245-based multimedia terminals) standard. This solution leverages Avaya Labs research and development efforts into a highly efficient encryption algorithm known as the Avaya Encryption Algorithm (AEA). Avaya has also openly embraced the National Institute of Standards and Technology (NIST) FIPS 197 Advanced Encryption Algorithm (AES). The FIPS 197 AES encryption algorithm has gone through an intensive public review process before being selected as the replacement for the Data Encryption Standard (DES).

The selection of an underlying encryption algorithm has to stand up to the highly demanding requirements of real time media streams which include scalability, end-point processing capacity and high tolerance to packet loss and re-ordering. The encryption-processing overhead must minimize CPU cycles and result in minimal latency and jitter. In non-technical terms this means that the differences in voice quality resulting from the encryption/decryption process must be imperceptible to the end-user. AEA and AES excel in these areas with a minimal 1-2 % increase in end-point processor utilization and less than 5ms added end-to-end latency. The encrypted media remarkably adds no additional IP overhead.

Avaya's pioneering implementation of Media Encryption offers the following benefits:

1. The ability to support end-to-end media encryption throughout the Avaya IP telephony endpoint portfolio.

Hardware	Minimum Software or Firmware to Support Media Encryption
Communication Manager	CM 1.3 >=
Avaya IP Phones:	
4601	R1.8
4602	R1.8
4606	R1.8
4610	R2.0
4612	R1.8
4620	R1.8
4624	R1.8
4630	R1.8
IP Softphone	R4V1 SP1
IP Softconsole	R1.5
IP Softphone for Pocket PC	R2.2
IP Agent	R5
TN2302AP IP Media Proc	V47
G350/G700 Media Gateways	V22

2. The flexibility to determine when to use AEA vs. AES. The Avaya Labs developed AEA encryption algorithm provides 104-bit RC-4 based encryption to the media stream. The Avaya implementation of the NIST FIPS 197 Advanced Encryption Algorithm (AES) uses a 128bit encryption key. As previously mentioned, AES is the replacement for DES.

The architectural implementation of Avaya media encryption allows for the addition of encryption algorithms and modes (cipher suites) as they are adopted in industry. Avaya's recent incorporation of the new federally approved AES algorithm demonstrates this extensibility. AES is implemented in a mode which is identical to that described in RFC 3711, Secure Real-Time Protocol. The addition of an authentication header as described in this RFC is planned for a future date. Administratively, customers are able to specify an encryption algorithm, just like they are able to specify different media codecs. No end-user involvement or adaptation is required to deploy media encryption and administrative configuration is very straight forward and requires no additional training.

To maintain system interoperability with third party products, Avaya media encryption is a configurable option and encryption algorithms can be ordered by usage preference. Avaya is committed to media privacy, and has taken the lead in offering media privacy with the necessary framework in place to readily support the standards based solutions of tomorrow.

Avaya media encryption capabilities have existed for well over three years, since DEFINITY Call Processing release 10. Avaya media encryption has been operating in real world mission critical environments and has field proven experience.

What separates Avaya from Competitive Offerings

Avaya's largest competitors in the IP Telephony marketplace either do not currently offer or do not offer the same extent of media encryption functionality. Only recently have certain vendors started offering media encryption capabilities and their early introductions are limited. Some of their key limitations in contrast to Avaya media encryption include:

1. Support is limited to newer model IP Telephones.

2. Support is limited to peer-to-peer IP media streams which excludes:

PSTN <-> IP media streams - Any time you make/receive a call from/to the PSTN, encryption of the IP portion of the call is turned off
Analog phone <-> IP media streams - when making/receiving a call within the campus - encryption of the IP portion of the call is turned off
Media streams between remote media gateways (one media server - distributed architecture) is not encrypted
Media streams between independent systems (media gateways controlled by independent media servers) is not encrypted
Media streams aggregated for conference calls are not encrypted
Questionable support for lawful observing of encrypted media communications (Communications Assistance for Law Enforcement Act/CALEA)

3. Implementation requires greater administrative effort (higher degree of complexity to set-up)

The Avaya Value Proposition

Avaya maintains a huge installed base of traditional telephony customers that have come to depend on the high reliability and security of their existing Avaya systems. The introduction of IP Telephony for many of these customers will be a migration process. Avaya has added the option for IP as an additional media transport mechanism while maintaining the feature rich call processing functionality and privacy customers has embraced, without sacrificing performance.

By proactively realizing and addressing the risks to voice privacy on a converged packet based network, Avaya has continued to demonstrate its awareness and commitment to highly reliable systems, privacy, and security. This effort has not gone unnoticed with Business Communication Review (BCR) noting, "Of all the IP-PBX vendors we've tested, Avaya exhibited the highest level of commitment to secure VOIP communications."