



VoIP Security and Privacy

**Making PC Platforms and
Networks Highly Secure**

Introduction

Voice over Internet Protocol (VoIP) offers many operational benefits over traditional PSTN calls, but with this technology comes additional concerns about security and privacy. Careful system design can address these issues and, in fact, make VoIP more secure and private than PSTN.

Potential benefits of VoIP include higher fidelity (wideband) audio, video, presence information, lower cost and improved manageability, all of which are made possible because VoIP travels over a flexible data network rather than the more confined circuit-switched network. However, the flexibility of this data network and its potential shared usage with other applications also adds levels of vulnerability. To address security and privacy concerns, the traffic not only needs to be encrypted effectively, but the distribution and storage of keys needs to be managed and the integrity of platforms verified. Ensuring network availability and quality of service are also important issues, but are beyond the scope of this paper.

When a PC hosts the VoIP client (sometimes called a software-phone or softphone), there are additional benefits from the integration, as well as additional threats. Benefits include use of the PC's resources and screen for video, file and document sharing, and rich integration with other applications, such as initiating a call from a calendar appointment. New vulnerabilities associated with the ability to interact with other applications include viruses, worms and spyware.

In fact, it is because VoIP clients are implemented on powerful platforms that more technology is available to provide robust security and privacy. Properly implemented, VoIP systems can be made more secure than the PSTN due to the availability of both communications security technology and platform security technology. This paper describes solutions for addressing security and privacy issues for VoIP networks and how to effectively address network vulnerabilities while maintaining platform integrity and performance.

Contents

Introduction	2
VoIP Network Security.....	3
Data Security	3
Infrastructure Security	3
Client Platform Security	4
Client Platform Integrity	4
Client Attestation	6
User Authentication.....	6
Key Management and Sealed Storage.....	7
Summary.....	7

VoIP Network Security

VoIP network security can be divided into two general categories: VoIP data security and VoIP infrastructure security. VoIP data security provides for privacy and integrity protection of VoIP media transmissions and includes end-user authentication of the remote party. VoIP infrastructure security encompasses protection of the network elements used to carry the VoIP traffic and protection of the signaling and network management traffic.

Data Security

End-to-end cryptographic protection of VoIP traffic over the public network provides privacy and integrity to VoIP conversations. There are a number of security protocols used for protection of VoIP data traffic. The most popular of these are Secure Real Time Protocol (SRTP)¹ and the IPSEC Encapsulating Security Payload (ESP)². Both of these protocols require cryptographic keys to be set up either dynamically through a separate key management protocol or manually. The Multimedia Internet KEYing (MIKEY)³ protocol is often used to exchange keys for use by SRTP, but it has not been universally adopted. For example, the draft *Session Description Protocol Security Descriptions*⁴ is sometimes used to exchange keying material and other elements of the cryptographic context. The IPSEC suite has its own native key exchange protocol called Internet Security Association and Key Management Protocol (ISAKMP).⁵

IPSEC is a more general layer 3 security protocol in that it can be used for many IP applications including VoIP. SRTP was designed specifically to protect VoIP (RTP) traffic and is more technically appropriate for the application than IPSEC.

Proper implementation of the security subsystem and protocols is more important than which particular security standard is chosen. (Assuming that the protocol and cryptographic algorithms that are chosen are based on well-established standards such as IPSEC or SRTP that have survived extensive peer review). Proper implementation dictates that security system issues, such as implementing a good randomizer and protecting the security system firmware from malicious or accidental modification, are comprehended, included in the design, and thoroughly tested. Proprietary security protocols are most likely more risky to use due to the fact that they do not have as much peer review and are therefore more likely to have undiscovered flaws.

Securely encrypting the signaling and the media is one of the ways that VoIP can be made more secure than PSTN. PSTN signaling and media are generally not encrypted, and most of the deployed phones and network equipment are incapable of encryption. PSTN predominately relies on physical security of the dedicated networks, but in many ways is vulnerable to eavesdropping or other attacks.

End-user authentication/traffic authentication is an end-to-end security service required to ensure that received VoIP traffic was sent by the expected party and to prevent masquerading. End-to-end authentication service is provided in key exchange protocols like ISAKMP and MIKEY or can be provided as a native part of the SIP⁶ signaling as discussed in the following section.

Infrastructure Security

Infrastructure security protects the VoIP network infrastructure from attack. VoIP network infrastructure consists of the network equipment used to signal, route, and provide management for VoIP services. Protection of the signaling and management communications also falls under the umbrella of infrastructure security.

Infrastructure Platform Security

Network infrastructure platform security is required to protect against cyber attacks and ensure the integrity of the network. It is important that the infrastructure equipment that implements the VoIP security functions is built upon platforms that are trusted and maintain software integrity. Recent news stories have disclosed vulnerabilities in network equipment that could be exploited to crash or remotely run malicious code. Such incidents highlight the need for platform assurance mechanisms such as those found in a technology that Intel has developed, code-named LaGrande.⁷ The subject of platform security and integrity is discussed further below.

Protection of Network Signaling

The use of common layer 3, 4 or application layer security encapsulation protocols such as IPSEC, TLS⁸(SSL) and S/MIME⁹ is the standard approach to protecting SIP signaling. Secure MIME (S/MIME) is a technology used to sign and encrypt standalone messages and allow recipients to verify and decrypt them. It was originally developed for protecting email but is also used to protect other types of messages, such as session descriptions, presence documents, and other data in the body of SIP message.

TLS, IPSEC and S/MIME protocols provide confidentiality and integrity protection of the signaling data. However, they do not provide end-to-end (client-to-client) protection of the signaling or internal signaling information elements. These encapsulating security protocols are terminated at each hop in the SIP network. Therefore the trust model for signaling is transitive hop-by-hop which is not as robust as an end-to-end trust model.

Work is being performed within the IETF SIP working group to specify end-to-end security mechanisms for the signaling of authenticable SIP identities. The draft *Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)*¹⁰ is an example of end-to-end security mechanisms embedded in the signaling protocol. Extending this type of approach to other portions of the VoIP signaling layer will enhance the security of the network.

The *Enhancements for Authenticated Identity* work also points to the need for a trust infrastructure that can issue authenticable credentials to VoIP end users (or to proxies trusted to vouch for their identities).

Identity and Trust Model

A trust infrastructure provides a level of confidence to the VoIP network interactions. The central part of a VoIP trust model is to provide a reasonable level of identity authentication and integrity for the network users. The trust infrastructure provides the facilities needed to assign and manage the identities of VoIP users and is part of the trust model.

The trust model dictates how identity certification services to VoIP network users and network providers are implemented. The trust infrastructure contains a Certification Authority (CA) that can issue cryptographically signed identity certificates or credentials to the users of the network. The digital signature of the CA can be verified by the network users who “trust” that the signed information issued by the CA is correct. These certificates are typically formatted in a digital certificate according to the ITU X.509¹¹ certificate standard. The trust model also defines what type of “proof of identity” information must be provided in order to get a certificate.

Another significant aspect of a trust model is management of platform trust, i.e., managing the assurance level of the devices that process VoIP traffic. Platform trust is distinct from user identity trust, although they share similar mechanisms, such as Certificate Authorities. For example, a CA could issue both user-identity certificates and device-identity certificates. Some type of standardized rating system to specify platform trust level could be developed so that a device CA has criteria to issue device credentials with.

Trust models can have different levels of identity granularity. For example, the identity information may only indicate the organization and department that the users (and platforms) are part of.

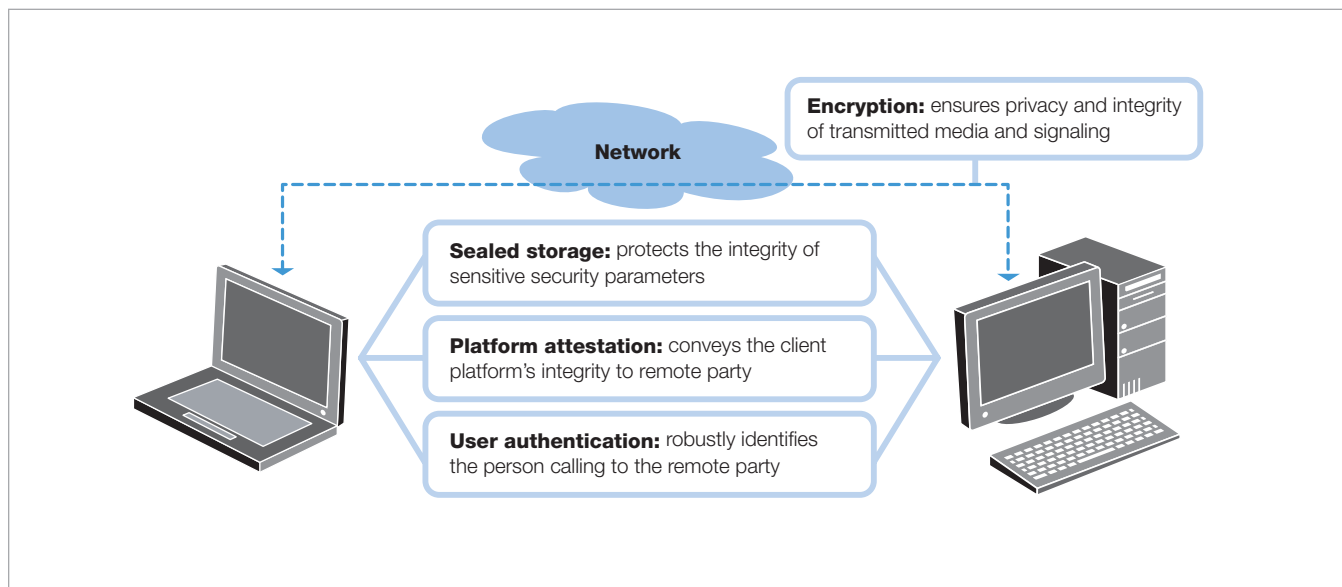
Platform trust and integrity are discussed in greater detail in Figure 1.

Client Platform Security

Client Platform Integrity

A concern for VoIP users is VoIP client platform security and integrity. A basic PSTN phone is a simple, single-purpose device, incapable of being remotely managed or upgraded, and therefore the device is not susceptible to network-based attacks.

Figure 1. Elements of platform trust and integrity.



A VoIP phone is a computer, whether an embedded, dedicated phone device or a general-purpose PC platform with VoIP software. These sophisticated, network-connected devices can, in most cases, be remotely managed and/or upgraded through the network. This provides powerful cost and time-saving advantages for both users and network managers, but it also means these devices may be vulnerable to malicious code that, for example, might install itself in the client platform to eavesdrop, record or log information about the calls made.

These platform security concerns are being addressed by forums such as the Trusted Computing Group and Intel has created technology, such as LaGrande Technology, to securely and efficiently realize these solutions. The goals of these activities are to harden the platform and prevent malicious software from being able to attack the software and get access to sensitive data. In fact, many of the following fundamental issues and solutions are not specific to VoIP, but are also relevant for protecting other data and applications as well.

Platform integrity prevents unauthorized software from eavesdropping on and/or compromising other software processes executing on the system. Platform security services can be used to protect the VoIP software running on a commodity PC or application specific VoIP platform from common Internet-based attacks such as viruses and spyware. Key technology being developed by Intel for providing platform-level security is LaGrande Technology (LT). The goal of LT is to protect the PC from software-based attacks.

LT features comprise capabilities in the microprocessor, chipset, I/O subsystems, and other platform components that are used to enforce the integrity of the platform, including:

Protected execution mechanisms for building protected software partitions

- These are used to provide a virtual firewall within the computer platform. Software contained in a protected partition cannot be maliciously modified or compromised by other software on the platform. A VoIP softphone that is configured in a protected partition is protected from other malicious software on the system. A secure virtualized platform can have a secure partition dedicated to the VoIP software and a separate partition that contains a commodity web browser and other untrusted software. This way, the platform user can surf the web while not compromising the VoIP software.

Sealed storage function

- This is used to protect sensitive parameters with hardware-based encryption and hardware key storage. A Trusted Platform Module (TPM) is a hardware device designed to securely store cryptographic key material used in platform authentication and other cryptographic functions. A TPM implements cryptographic keys used for digital signatures and key wrapping in hardware. LT makes use of a TPM for platform attestation (discussed on page 6). A TPM can be used to securely store key material that protects VoIP communications.

Figure 2 depicts the basic platform security components of a trusted VoIP Softphone discussed in this paper. These components include a secure execution environment; a high-assurance hardware-based cryptographic module, and a Trusted Platform Module.

Client Attestation

Proof of platform integrity is a security service that allows a remote system to verify the integrity level of a system that it connects to. This service and the associated protocols are being defined in the Trusted Computing Group's Trusted Network Connect Working Group. Remote platform integrity verification is accomplished using a mechanism called attestation whereby the remote platform provides an electronically signed digest of its operating environment or the description of platform characteristics that affect the integrity of the platform. As discussed earlier, TLS is one of the security protocols used in VoIP systems to provide security to the SIP signaling for VoIP sessions. TLS Extensions for Attestation¹² is used to exchange platform integrity and authentication information as part of the security exchange between VoIP entities.

Proof of platform integrity could be used by communicating VoIP platforms to verify the robustness of the remote party's platform. It is conceivable that the users would restrict the information they share based upon the integrity level of the remote VoIP phone.

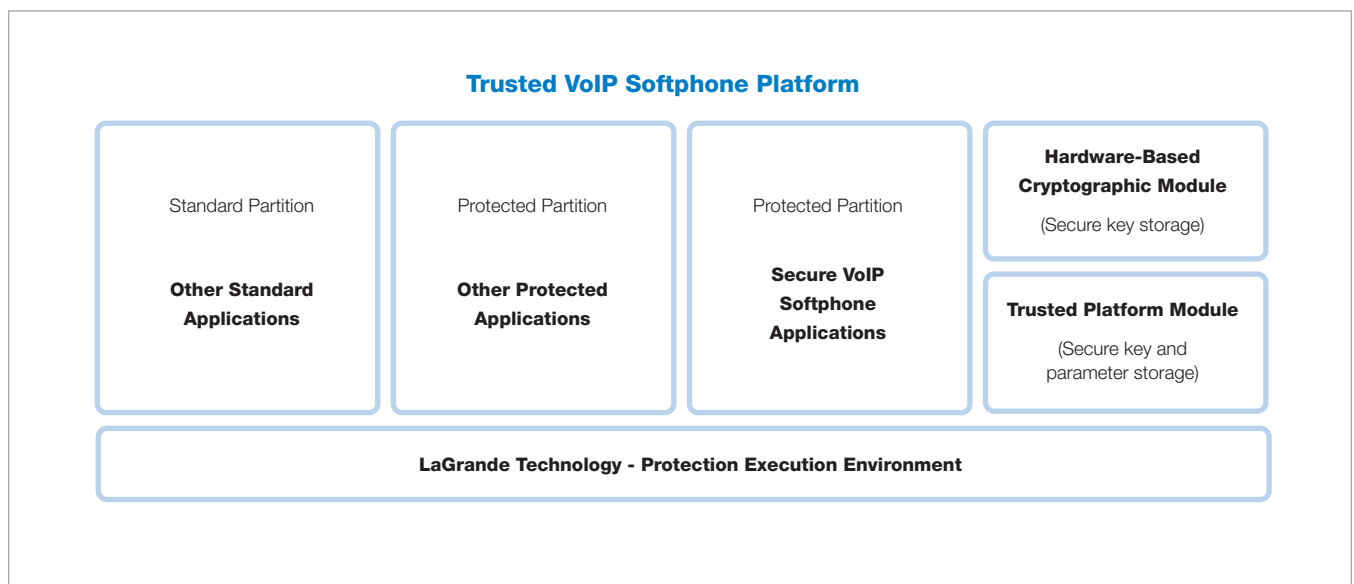
The remote party's platform integrity level would be displayed in some fashion as part of call establishment so that a decision could be made about whether to accept or reject the call or restrict what is communicated based upon the level. This integrity level information could be thought of in the same manner as the security level (128 bit, 64 bit) of the security protocol and key size that is negotiated during call setup. It is these two pieces of information and the key management system that really define how secure the end-to-end link is. There would have to be standardized criteria and minimal essential requirements for each integrity level. Businesses could establish employee policies that state which integrity level is required to discuss certain types of information. Consumers could make their own choices based on how they perceive the threat of communicating with a low integrity VoIP phone.

In addition to authenticating the remote party's platform, user-authentication can identify the remote party.

User Authentication

A PSTN phone relies on physical security for caller identification. Anyone who is within reach of the phone, or can physically access the network, can masquerade and answer or place a call. In contrast, VoIP phones can be designed with additional security measures to authenticate the user, which may include passwords, biometric input, or combinations. Furthermore,

Figure 2. The basic platform security components of a trusted VoIP Softphone. These components include a secure execution environment, a high-assurance hardware-based cryptographic module, and a Trusted Platform Module.



this identity can then be sent securely through the network to the other party using digital signature techniques described in the “*Enhancements for Authenticated Identity*” draft.

The proper use of these platform-attestation and user-authentication technologies will enable the design of secure VoIP platforms that provide many more security services than are provided in their PSTN counterpart.

Key Management and Sealed Storage

The various encryption protocols mentioned previously require key management: the generation, storage, protection, and destruction of cryptographic keying material. Proper key management is essential in the design of any cryptographic security system. Key management is critical in applications such as VoIP where any-to-any communications can be established on the fly.

Secure key storage is essential because adversaries will typically not try to break a strong cryptographic algorithm, such as 3DES¹³ or AES.¹⁴ Rather, they will try to exploit vulnerability in the security implementation, such as gaining access to the cryptographic key material that is used to authenticate and protect the VoIP sessions. Spyware attacks that search for key material on a client device can compromise all of the VoIP sessions made on the system. Hardware-based key storage, as well as protection of key material throughout its lifetime, is an essential security requirement. FIPS-140-2

level 3 and higher certified cryptographic modules or devices such as the Trusted Platform Module that provide hardware-based key storage provide the type of key protection required to prevent key extraction type attacks. At the Intel Developer Forum in March 2005, Intel demonstrated a secure system that used TPM to store keys for SRTP.

Summary

The sophistication of VoIP clients and network components allow IP-based telephony systems to offer many features that are not economically feasible with PSTN-based systems. This sophistication brings additional vulnerabilities that must be addressed. Properly applied security measures can make VoIP communications more secure and private than PSTN communications. Whereas PSTN relies on the physical security of the network, VoIP can encrypt signaling and media end-to-end. Mechanisms for securing the client platform and for attestation of the client’s integrity also enhance VoIP security. In addition, VoIP also provides a means of user authentication, whereas PSTN relies predominantly on physical access to the phone.

There are many aspects of VoIP security, and well-known ways to robustly implement each of them. Properly applied, VoIP can provide richer and more secure communication than PSTN.

¹ Baugher, M., McGrew, D., Naslund, M., Carrara, E., and Norman, K., “The Secure Real-time Transport Protocol (SRTP),” RFC 3711, March 2004.

² Kent, S. and Atkinson, R., “IP Encapsulating Security Payload (ESP),” RFC 2406, November 1998.

³ Arkko, J., Carrara, E., Lindholm, F., Naslund, M. and Norman, K., “MIKEY: Multimedia Internet KEYing”, RFC 3830, August 2004.

⁴ Andreasen, F., Baugher, M. and Wing, D., “Session Description Protocol Security Descriptions for Media Streams”, draft-ietf-mmusic-sdescriptions-12, September, 2005.

⁵ Maughan, D., Schertler, M., Schneider, M. and Turner, J., “Internet Security Association and Key Management Protocol (ISAKMP),” RFC 2408, November 1998.

⁶ Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and Schooler, E., “SIP: Session Initiation Protocol”, RFC 3261, June 2002.

⁷ Intel Corporation, “LaGrande Technology Architectural Overview”, 252491-001, avail. at <http://www.intel.com/technology/security/>, September 2003.

⁸ Dierks, T. and Allen, C., “The TLS Protocol Version 1.0”, RFC 2246, January 1999.

⁹ Ramsdell, B., “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification”, RFC 3851, July 2004.

¹⁰ Peterson, J and Jennings, C., “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)”, Internet-Draft draft-ietf-sip-identity-06, October 2005.

¹¹ International Telecommunications Union, “Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks”, ITU-T Recommendation X.509, ISO Standard 9594-8, March 2000.

¹² Trusted Computing Group, TLS Extensions for Attestation, Specification Version 1.0, Revision 0.8, July 2004, Work in Progress.

¹³ National Institute of Standards and Technology, “Data Encryption Standard,” FIPS PUB 46-2, December 1993.

¹⁴ National Institute of Standards and Technology, “Advanced Encryption Standard (AES),” FIPS PUB 197, November 2001.



Copyright © 2005 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Information in this document is provided in connection with Intel® products. Except as provided in Intel's terms and conditions of sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty relating to sale and/or use of Intel products, including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright, or other intellectual property right. Intel may make changes to specifications, product descriptions, and plans at any time, without notice.

Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights. Intel products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications. The Intel® Pentium® M processor and the Intel® Celeron® M processor may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available upon request.