Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 14 Issue 2 Version 1.0 Year 2014
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Voip End-To-End Security using S/MIME and a Security Toolbox

By Md. Shahidul Islm

Rajshahi University of Engineering & Technology, Bangladesh

Abstract- Voice Over Internet Protocol (VOIP) is a rapidlygrowing Internet service for telephone communication. However, while it offers a number of cost advantages over traditional telephone service, it can pose a security threat, especially when used over public networks. In the absence of sufficient security, users of public networks are open to threats such as identity theft, man-in-the-middle attack, interception of messages/eavesdropping, DOS attacks, interruption of service and spam. S/MIME adds security to the message itself and can be used to provide end-to-end security to SIP. S/MIME can also offer confidentiality or integrity, or both, but it does not provide any anti-replay protection. However, we propose to use a unified architecture for the implementation of security protocols in the form of a security toolbox system. It will prevent an attack against anti-replay.

Keywords: S/MIME, SIP, IPSEC, replay attack, SDP.

GJCST-E Classification : C.2.0

Voip End-To-End Security using S/MIME and a Security Toolbox

Md. Shahidul Islm

Abstract- Voice Over Internet Protocol (VOIP) is a rapidly-growing Internet service for telephone communication. However, while it offers a number of cost advantages over traditional telephone service, it can pose a security threat, especially when used over public networks. In the absence of sufficient security, users of public networks are open to threats such as identity theft, man-in-the-middle attack, interception of messages/eavesdropping, DOS attacks, interruption of service and spam. S/MIME adds security to the message itself and can be used to provide end-to-end security to SIP. S/MIME can also offer confidentiality or integrity, or both, but it does not provide any anti-replay protection. However, we propose to use a unified architecture for the implementation of security protocols in the form of a security toolbox system. It will prevent an attack against anti-replay.

Keywords: S/MIME, SIP, IPSEC, replay attack, SDP.

I. Introduction

How can a client be sure that his message will not be intercepted by someone? This is the most important and urgent question that security professionals have to answer when dealing with VoIP systems.

Voice over Internet Protocol is a rapidly growing Internet service. Voice over IP (VoIP) has been developed in order to provide access to voice communication anywhere in the world. VoIP is simply the transmission of voice conversations over IP-based networks. Although IP was originally planned for data networking, now it is also commonly used for voice networking. While VoIP (Voice over Internet Protocol) offers a number of cost advantages over traditional telephoning, it can also pose a security threat. So watertight security is needed when using VoIP, end-to-end, especially when used on a public network. There is, however, no standard for VoIP and no general solution for VoIP security. The security of VoIP systems today is often non-existent or, in the best case, weak. As a result, hackers can easily hack.

II. Review

Several writers have taken on this or similar problems. Gupta and Shmatikov [1] investigated the security of the VoIP protocol stack, as well as SIP, SDP, ZRTP, MIKEY, SDES, and SRTP. Their investigation found a number of flaws and opportunity for replay attacks in SDES that could completely smash content protection. They showed that a man-in-the-middle attack was possible using ZRTP. They also found a weakness in the key derivation process used in MIKEY.

Niccolini et al. [2] designed an intrusion prevention system architecture for use with SIP. They evaluated the effectiveness of legitimate SIP traffic in the presence of increasing volumes of malformed SIP INVITE messages in an attack scenario.

Fessi et al. [3] proposed extensions to P2P SIP and developed a signaling protocol for P2P SIP that uses two different Kademlia-based overlay networks for storing information and forwarding traffic. Their system requires a centralised authentication server, which provides verifiable identities at the application/SIP layer.

Palmieri and Fiore [4] describe an adaptation of SIP to provide end-to-end security using digital signatures and efficient encryption mechanisms. The authors developed a prototype implementation and conducted a performance analysis of their scheme. However, one weakness of this system is that it is open to man-in-the-middle attacks.

Syed Abdul and Mueed Mohd Salman [5] developed Android driven security in SIP based VoIP systems using ZRTP on GPRS network. It communicated securely, using the GPRS data channel encrypted by using ZRTP technique. As it relies on ZRTP, it is probably vulnerable to man-in-the-middle attacks too.

Chirag Thaker, Nirali Soni and Pratik Patel [6] developed a new Performance Analysis and Security Provisions for VoIP Servers. This paper provided a performance analysis of VoIP-based servers providing services like IPPBX, IVR, Voice-Mail, MOH, Video Call and also considered the security provisions for securing VoIP servers.

III. Related Work

This paper considers a different solution, presenting a structure to assure end-to-end security by using the key management protocol S/MIME with the security toolbox system. S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. S/MIME provides end-to-end integrity, confidentiality protection and does not require the intermediate proxies to be trusted. However, S/MIME does not provide any anti-replay protection. To protect against a replay attack, we use

Author: Rajshahi University of Engineering & Technology (RUET) DEP: ETE, Rajshahi, Bangladesh. e-mail: sohidsakir@gmail.com

the security toolbox system. Toolbox system is a protocol as a single package comprised of two layers: control and a library of algorithms.

IV. Parameters' of a Solution

SIP is an application-layer protocol standardized by the Internet Engineering Task Force (IETF), and is designed to support the setup of bidirectional communication sessions for VoIP calls. The main SIP entities are endpoints (softphones or physical devices), a proxy server, a registrar, a redirect server, and a location server.

However, TLS (Transport Layer Security) can be used to introduce integrity and confidentiality to SIP between two points. Although it uses SIP signaling to secure, it has some limitations. Each proxy needs the SIP header in clear text to be able to route the message properly. All proxies in use in a connection must be trusted, as messages are decrypted and encrypted in each node. There will be no assurance that an SIP message cannot be intercepted by someone in the network.

IPSec can also be used to provide confidentiality, integrity, data origin authentication and even replay protection to SIP. It cannot be used in end-to end security. Proxy servers need to read from SIP headers and sometimes write to them. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host). IPSec assumes, however, that a pre-established trust relationship has been introduced between the communicating parties, making it most suited for SIP hosts in a VPN scenario. Further, the SIP specification does not describe how IPSec should be used; neither does it describe how key management should be operated.

S/MIME is a set of specifications for securing electronic mail and can also be used to secure other applications such as SIP. S/MIME provides security services such as authentication, non-repudiation of origin, message integrity, and message privacy. Other security services include signed receipts, security labels, secure mailing lists, and an extended method of identifying the signer's certificate(s) etc.

S/MIME provides open, interoperable protocols that allow compliant software to exchange messages that are protected with digital signatures and encryption. S/MIME requires that each sender and recipient have an X.509-format digital certificate, so public-key infrastructure (PKI) design and deployment is a major part of S/MIME deployment.

The same mechanisms can be applied for SIP. The MIME security mechanism is referred to as S/MIME and is specified in RFC 2633. S/MIME adds security to the message itself and can be used to provide end-to-end security to SIP.

Suppose two clients are trying to communicate each other. One client wants to send a message to the other client.

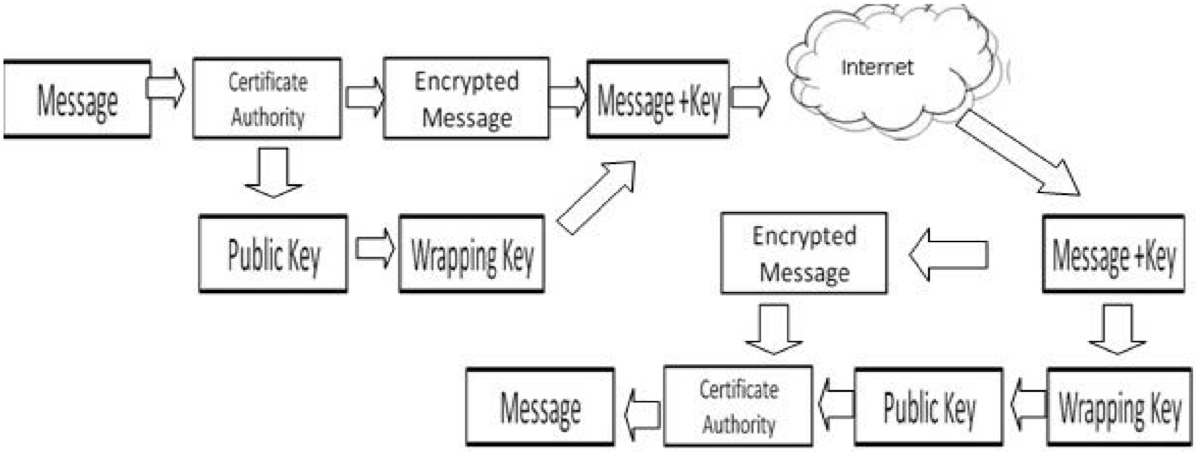

Figure 2 : End-to-end security

Figure 1 shows how to send the message in secure way. Before S/MIME can be used to encrypt the message, one needs to obtain a key/certificate, either from one's in-house certificate authority (CA) or from a public CA.

The client uses S/MIME to sign and/or encrypt a SIP message. S/MIME combines public-key and secret-key cryptography. To encrypt the message, the sender obtains certificates from the certificate authority (CA) and generates a strong, random secret key. The message is then signed with the private key of the sender.

The encryption of the message is a bit trickier. It requires that the public key of the recipient is known to the sender. This key must be fetched in advance or be fetched from some kind of central repository. The secret key is used to encrypt the message, and then the public key of the recipient is used to encrypt the key for the recipient. When the recipient gets the message, he uses the private key to decrypt his copy of the secret key, and the secret key is used to decrypt the original message.

V. The Security Risk

S/MIME does not provide any anti-replay protection. The most serious attack is a replay attack on SDES, which causes SRTP to repeat the key stream used for media encryption, thus completely breaking transport-layer security. To protect against a replay attack, we use the security toolbox. How to use it to prevent an attack on SRTP, when used in combination with an SDES key exchange, is described below.

Suppose two users, Alice and Bob are trying to communicate with each other. Bob is the initiator in this session, and SDES is used to transport SRTP key material. To provide confidentiality for the SDES message, S/MIME is used to encrypt the payload.

S/MIME does not provide any anti-replay protection. Suppose an attacker, Charles, is trying to attack the call. Charles sends the copy of Bob's original INVITE message to Alice, containing an S/MIME-encrypted SDP attachment, with the SDES key transfer message. Since Alice does not maintain any state for SDP, she will not be able to detect the replay. Charles will effectively, for Alice, become Bob!

This is why it is proposed to use security toolbox: to prevent such a personation attack. Since anti-replay tools will be maintained all states for SDP, at all times, all messages will be filtered through anti-replay tools. Anti-replay tools will be able to detect the replay. S/MIME provides the security at the document level and IPSec performs the same function at the packet level. This configuration should become common whenever an application uses S/MIME as a document-level protection.

VI. A Security Toolbox

Ibrahim S. Abdullah and Daniel A. Menasce [9] designed a security toolbox. In the toolbox, every tool carries out a specific function such as: encryption, decryption, random number generation, integrity protection, anti-replay, and header processing.

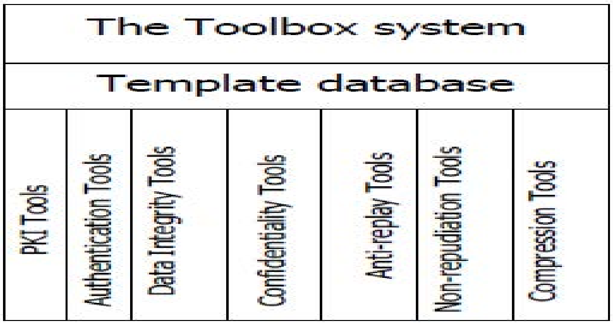

Figure 2 : Components of A Toolbox System

Figure 2 shows the major components of such a toolbox. The template is a set of specifications that define the required security services. The template database takes the necessary steps from the database for overall protection.

The toolbox architecture consists of two parts: one that must be secured as part of the trusted domain of the operating system (CBT) and another that may be part of the user domain.

The secure part consists of the following components:

1. Databases: store information about different operations of the toolbox, such as: private and secret keys, templates, registry for the tools and template names, alert messages, authorization information, policies, and the toolbox configuration information.
2. Interpretation engine: interprets protocol templates.
3. Security tools: the set of tools that implement the security algorithms.
4. Cache: stores temporary keys and associated information.
5. Inter-communication manager: handles control messages between toolboxes running at different hosts (e.g., during handshake).

The second part of the toolbox consists of:

a) Template developer and analyser: analyses template creation, verification, and maintenance.
b) Certificate repository: contains copies of the certificates that the toolbox consults for authentication. These certificates may be placed in public storage, because they are protected by their creator's digital signature. This repository could part of a directory service application.
c) Directory services are standard applications used to provide user's authentication and authorization services.

Now let us revisit our friends Alice and Bob with a security toolbox. Recall that Bob accepts Alice's INVITE message. They communicate but then Charles sends replay messages to Alice, pretending to be Bob. Now the security toolbox takes action. First, the toolbox, working with IPSec, has full identification of Bob: especially including his IP Packets. When Charles starts to copy Bob's messages and send them as if he were Bob, the toolbox sees that Charles' IP Packet is not the same as Bob's. Therefore, Charles is recognized as a personator and his packets are denied access to Alice. Charles' scheme fails and he goes away with nothing. Alice and Bob continue to communicate happily without any interference from hackers like Charles.

VII. Conclusion

S/MIME is being increasingly used as at security system for VoIP messages. However, S/MIME has an Achilles heel. The Achilles heel is the replay attack. This happens because S/MIME does not identify the source of the messages coming into the system. This article suggests a solution to this problem by combining the S/MIME with a security toolbox, using IPSec to monitor IP packet. The toolbox monitors the IP packet of message originators and, where a new IP address enters from the same source, denies access to the message. Such a solution guarantees complete end-to-end user security for VoIP messages at minimal cost. Thus S/MIME, with this solution, maximizes effectiveness, given the technology of the moment, in protecting the user.

References Références Referencias

1. P. Gupta and V. Shmatikov(2007), Security Analysis of Voice-over-IP Protocols. In Proceedings of the 20th IEEE Computer Security Foundations Symposium (CSFW), pages 49–63.
2. M. Petraschek, T. Hoeher, O. Jung, H. Hlavacs, and W. N. Ganstere(2008), Security and Usability Aspects of Man-in-the-Middle Attacks on ZRTP, Journal of Universal Computer Science, vol. 14, no. 5, pp. 673– 692.
3. S. Niccolini, R. G. Garroppo, S. Giordano, G. Risi, and S. Ventura(2006), SIP Intrusion Detection and Prevention: Recommendations and Prototype Implementation. In Proceedings of the 1st IEEE Workshop on VoIP Management and Security (VoIP MaSe), pages 47–52.
4. A Fessi, N. Evans, H. Niedermayer, and R. Holz(2010), Pr2-P2PSIP: Privacy Preserving P2P Signaling for VoIP and IM, in Proceedings of the 4th Annual ACM Conference on Principles, Systems and Applications of IP Telecommunications (IPTCOMM), pp. 141–152.
5. F. Palmieri and U. Fiore(2009), Providing True End-to-End Security in Converged Voice over IP Infrastructures, Computers & Security, vol. 28, pp. 433–449.
6. Jim Murphy(2013), Toll Fraud Challenges and Prevention in a VoIP Environment (President of Phone Power).
7. Syed Abdul Mueed, Mohd Salman(2012), Android driven security in SIP based VoIP systems using ZRTP on GPRS network.(International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No.2)
8. Jonathan Zar, David Endler and Dipak Ghosal(2005) VoIP Security and Privacy Threat Taxonomy (VIOPSA).
9. Ibrahim S. Abdullah and Daniel A. Menasce(2003), A unified architecture for the implementation of security protocols. In the Proc. of Computer Applications in Industry and Engineering (CAINE03), Las Vegas, Nevada USA, 11-13.