ISSN: 2321-7782 (Online)
Volume 1, Issue 7, December 2013
International Journal of Advance Research in Computer Science and Management Studies
Research Paper
Available online at: www.ijarcsms.com

A Noval Approach for S/MIME

K.Suganya
Associate Professor
Department of Software Engineering & IT [PG]
A.V.C College of Engineering
Mayiladuthurai - India

Abstract: Email Communication is insecure. Emails can be read and modified as they are passed through the Internet as clear-Text .S/MIME is an attempt to standardize a protocol used to encrypt and digitally sign email correspondence. S/MIME can be used in automated message transfer agents that use cryptographic security services that do not require any human intervention, such as the signing of software generated documents and encryption of FAX messages sent over the internet.

Keyword: IETF, PKCS, RSA, CA, SMTP, HTTP.

I. INTRODUCTION

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of e-mail encapsulated in MIME. It is on an IETF standards track and defined in a number of documents, most importantly RFCs. S/MIME was originally developed by RSA Data Security Inc. The original specification used the recently developed IETF MIME specification with the de facto industry standard PKCS #7 secure message format. Change control to S/MIME has since been vested in the IETF and the specification is now layered on Cryptographic Message Syntax, an IETF specification that is identical in most respects with PKCS #7.

S/MIME (Secure / Multipurpose Internet Mail Extensions) is a protocol that adds digital signatures and encryption to Internet MIME (Multipurpose Internet Mail Extensions) messages described in RFC 1521. MIME is the official proposed standard format for extended Internet electronic mail. Internet e-mail messages consist of two parts, the header and the body. The header forms a collection of field/value pairs structured to provide information essential for the transmission of the message. The structure of these headers can be found in RFC 822. The body is normally unstructured unless the e-mail is in MIME format. MIME defines how the body of an e-mail message is structured. The MIME format permits e-mail to include enhanced text, graphics, audio, and more in a standardized manner via MIME-compliant mail systems. However, MIME itself does not provide any security services.

The purpose of S/MIME is to define such services, following the syntax given in PKCS #7 for digital signatures and encryption. The MIME body section carries a PKCS #7 messages, which itself is the result of cryptographic processing on other MIME body sections. S/MIME standardization has transitioned into IETF, and a set of documents describing S/MIME version 3 have been published there. S/MIME has been endorsed by a number of leading networking and messaging vendors, including ConnectSoft, Frontier, FTP Software, Qualcomm, Microsoft, Lotus, Wollongong, Banyan, NCD, SecureWare, VeriSign, Netscape, and Novell.

© 2013, IJARCSMS All Rights Reserved

II. S/MIME HISTORY

S/MIME was developed by RSA Data Security to thwart forgery and interception of electronic messages. S/MIME was created on the existing MIME protocol standard and it can be integrated easily into the existing email and messaging products. As S/MIME was designed on the existing popular supported standards, it became quite popular and was implemented across a wide range of operating systems and email clients. Another reason for the S/MIME protocol's wide acceptance is that S/MIME allows a Windows user to send a digitally signed and secure email with the Outlook email client to a Unix OS user, who can receive the email using the Netscape email client. The users do not have to install any additional program or software to utilize this facility.

III. S/MINE IN CRYPTOGRAPHY

The S/MIME format is the IETF RFC 2311 specification for encrypting and signing message data. This format creates one-way hash algorithms that ensure data integrity by verifying that no modifications are made to a message while in transit. The sender's identity is validated using a digital signature. S/MIME is the encryption-supported version of the MIME protocol, based on Public Key Cryptography Standards (PKCS).

PKCS standards specify how RSA Data Security public-key cryptographic algorithms are used to implement enveloped encryption and digital signatures. The RSA public-key system uses two related keys to perform the mathematical algorithms that encrypt and decrypt data: a public key, which may be made available to any prospective correspondent, and a private key known only to the key's owner, for example:

A public key can be published openly, allowing anyone to send secure messages that can only be decrypted by the owner of the private key. Public keys are stored as certificates that comply with the X.509 standard. In addition to the public key, a certificate also contains information about the key owner's identity, the key's validity, and the CA that issued the certificate.

Private Key encryption can be decrypted with a corresponding public key. This encryption method creates a digital signature, which guarantees that the signed message is authentic and came from the originator.

Digital signatures provide data integrity, authentication and nonrepudiation of electronic documents. Digital signature verification ensures that: The document received is identical to the document sent. There is authentication of the identity of the sender. No subsequent repudiation of the document by the originator occurs.

IV. HOW S/MIME WORKS

The S/MIME standard is based on the principle of public-key encryption. S/MIME therefore makes it possible to encrypt the content of messages but does not encrypt the communication.

The various sections of an electronic message, encoded according to the MIME standard, are each encrypted using a session key.

The session key is inserted in each section's header, and is encrypted using the recipient's public key. Only the recipient can open the message's body, using his private key, which guarantees the confidentiality and integrity of the received message.

In addition, the message's signature is encrypted with the sender's private key. Anyone intercepting the communication can read the content of the message's signature, but this ensures the recipient of the sender's identity, since only the sender is capable of encrypting a message (with his private key) that can be decrypted with his public key.

S/MIME version 2 is defined in RFC 2311 (S/MIME Version 2 Message Specification, March 1998) and RFC 2312 (S/MIME Version 2 Certificate Handling, March 1998). S/MIME v2 was considered as an IETF standard, but was rejected

© 2013, IJARCSMS All Rights Reserved

because the IETF felt that it was encumbered by patents held by RSA Data Security. In addition, S/MIME v2 used weak 40-bit key cryptography.

The IETF standardized S/MIME version 3 in 1999. This version is defined in RFC 2632 (S/MIME Version 3 Certificate Handling, June 1999), RFC 2633 (S/MIME Version 3 Message Specification, June 1999), and RFC 2634 (Enhanced Security Services for S/MIME, June 1999).

S/MIME v3 provides authentication, message integrity and nonrepudiation of origin (via digital signatures), and privacy and data security (via encryption). S/MIME is normally used to secure outgoing mail and interpret incoming secure mail. It may also be used to secure data across HTTP links. S/MIME v3 cryptographically enhances MIME body parts according to CMS (cryptographic message syntax), which is described in RFC 2630 (Cryptographic Message Syntax, June 1999). The Cryptographic Message Syntax describes an encapsulation syntax for data protection.

Function

S/MIME provides the following cryptographic security services for electronic messaging applications: authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy and data security (using encryption). S/MIME specifies the application/pkcs7-mime (smime-type "enveloped-data") type for data enveloping (encrypting): the whole (prepared) MIME entity to be enveloped is encrypted and packed into an object which subsequently is inserted into an application/pkcs7-mime MIME entity.S/MIME functionality is built into the vast majority of modern e-mail software and interoperates between them.

S/MIME Certificates

Before S/MIME can be used in any of the above applications, one must obtain and install an individual key/certificate either from one's in-house certificate authority (CA) or from a public CA such as one of those listed below. Best practice is to use separate private keys (and associated certificates) for Signature and for Encryption, as this permits escrow of the encryption key without compromise to the non-repudiation property of the signature key. Encryption requires having the destination party's certificate on store (which is typically automatic upon receiving a message from the party with a valid signing certificate). While it is technically possible to send a message encrypted (using the destination party certificate) without having one's own certificate to digitally sign, in practice, the S/MIME clients will require you install your own certificate before they allow encrypting to others.

A typical basic personal certificate verifies the owner's identity only in terms of binding them to an email address and does not verify the person's name or business. The latter, if needed (e.g. for signing contracts), can be obtained through CAs that offer further verification (digital notary) services or managed PKI service. For more detail on authentication, see Digital Signature.

Depending on the policy of the CA, your certificate and all its contents may be posted publicly for reference and verification. This makes your name and email address available for all to see and possibly search for. Other CAs only post serial numbers and revocation status, which does not include any of the personal information. The latter, at a minimum, is mandatory to uphold the integrity of the public key infrastructure.

V. SECURITY SERVICES FOR S/MIME

S/MIME provides two security services: Digital signatures & Message encryption

These two services are the core of S/MIME-based message security. All other concepts related to message security support these two services. Although the full scope of message security may seem complex, these two services are the basis of message security.

© 2013, IJARCSMS All Rights Reserved

- ***Digital Signature in S/MIME***

Digital signatures are the more commonly used service of S/MIME. digital signatures provide the following security capabilities:

- **Authentication** A signature serves to validate an identity. It verifies the answer to "who are you" by providing a means of differentiating that entity from all others and proving its uniqueness. Because there is no authentication in SMTP e-mail, there is no way to know who actually sent a message. Authentication in a digital signature solves this problem by allowing a recipient to know that a message was sent by the person or organization who claims to have sent the message.

- **Nonrepudiation** The uniqueness of a signature prevents the owner of the signature from disowning the signature. This capability is called nonrepudiation. Thus, the authentication that a signature provides gives the means to enforce nonrepudiation. The concept of nonrepudiation is most familiar in the context of paper contracts: a signed contract is a legally binding document, and it is impossible to disown an authenticated signature. Digital signatures provide the same function and, increasingly in some areas, are recognized as legally binding, similar to a signature on paper. Because SMTP e-mail does not provide a means of authentication, it cannot provide nonrepudiation. It is easy for a sender to disavow ownership of an SMTP e-mail message.

- **Data integrity** An additional security service that digital signatures provide is data integrity. Data integrity is a result of the specific operations that make digital signatures possible. With data integrity services, when the recipient of a digitally signed e-mail message validates the digital signature, the recipient is assured that the e-mail message that is received is, in fact, the same message that was signed and sent, and has not been altered while in transit. Any alteration of the message while in transit after it has been signed invalidates the signature. In this way, digital signatures are able to provide an assurance that signatures on paper cannot, because it is possible for a paper document to be altered after it has been signed.

- ***Message Encryption in S/MIME***

Message encryption provides a solution to information disclosure. SMTP-based Internet e-mail does not secure messages. An SMTP Internet e-mail message can be read by anyone who sees it as it travels or views it where it is stored. These problems are addressed by S/MIME through the use of encryption.

Encryption is a way to change information so that it cannot be read or understood until it is changed back into a readable and understandable form.

Although message encryption is not as widely used as digital signatures, it does address what many perceive as the most serious weakness in Internet e-mail. Message encryption provides two specific security services:

- **Confidentiality** Message encryption serves to protect the contents of an e-mail message. Only the intended recipient can view the contents, and the contents remain confidential and cannot be known by anyone else who might receive or view the message. Encryption provides confidentiality while the message is in transit and in storage.

- **Data integrity** As with digital signatures, message encryption provides data integrity services as a result of the specific operations that make encryption possible.

VI. CONCLUSION

S/MIME is being supported by popular e-mail software such as Microsoft Outlook, Outlook Express and Netscape Messenger. With the recent signature laws providing a legal infrastructure for signed e-mail correspondence within the European Union and increased e-mail surveillance providing the need for encryption, it is obvious that secure e-mail processing

© 2013, IJARCSMS All Rights Reserved

will get more attention in the future than it gets now. Security of operating system and e-mail mechanisms are beyond the scope of this profile. For example, system operators must ensure that the operating system itself is secured; and that the e-mail system is secure. This profile addresses only the security aspects of IETF developed S/MIME extensions.

References

1. William Stallings, "Cryptography and Network Security: Principles and Practice, Second Edition." Upper Saddle River, NJ: Prentice Hall, 1999.
2. RSA Security, Inc., "Public-Key Cryptography Standards", http://www.rsasecurity.com/rsalabs/pkcs/index.html
3. N. Borenstein, N. Freed, "MIME (Multipurpose Internet Mail Extensions) Part One (RFC 1521)", http://www.ietf.org/rfc/rfc1521.txt
4. Internet Mail Consortium, "S/MIME and OpenPGP", http://www.imc.org/smimepgpmime.Html
5. http://www.javvin.com/protocol/rfc2045.pdf : Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies
6. http://www.javvin.com/protocol/rfc2046.pdf : Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types
7. http://www.javvin.com/protocol/rfc2047.pdf :MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text
8. http://www.javvin.com/protocol/rfc2048.pdf : Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures.
9. http://www.javvin.com/protocol/rfc2049.pdf : Multipurpose Internet Mail Extensions
10. http://www.javvin.com/protocol/rfc2632.pdf : S/MIME Version 3 Certificate Handling
11. http://www.javvin.com/protocol/rfc2633.pdf : S/MIME Version 3 Message Specification
12. D. Atkins, W. Stallings, P. Zimmermann, "PGP Message Exchange Formats (RFC 1991)", http://www.ietf.org/rfc/rfc1991.txt
13. Callas, L. Donnerhacke, H. Finney, R. Thayer, "OpenPGP Message Format (RFC 2440)",http://www.ietf.org/rfc/rfc2440.txt
14. Brian Fonseca, "VeriSign issues false Microsoft digital certificates", InfoWorld, March 22, 2001,http://infoworld.com/articles/hn/xml/01/03/22/010322hnmicroversign.xml
15. Simson Garfinkel, "Pretty Good Politics",http://hotwired.lycos.com/packet/garfinkel/97/18/index2a.html
16. Ed Gerck, "Overview of Certification Systems", July 18, 2000,http://www.mcg.org.br/certover.pdf
17. Internet Mail Consortium, "S/MIME and OpenPGP", http://www.imc.org/smimepgpmime.html
18. Kevin McCurley, "DigiCrime is now known as root@localhost",http://www.digicrime.com/id.html
19. "Official Internet Protocol Standards", http://www.rfc-editor.org/rfcxx00.html
20. OpenPGP Alliance, http://www.openpgp.org/about_openpgp/history.shtml

AUTHOR(S) PROFILE

K.Suganya, is presently working as a associate professor in A.V.C College of Engineering, Mayiladuthurai, India, and she is having ten years of experience in the same institution. Her interested area is network security and Cryptography.

© 2013, IJARCSMS All Rights Reserved