Evolution of Email Security Standards

Russell Housley, Vigil Security, LLC

Abstract

The first work on email security began in 1984, which resulted in the Privacy Enhanced Mail (PEM) specifications. Two years later, work was done as part of the Secure Data Network System (SDNS) sponsored by the U.S. Government, resulting in the Message Security Protocol (MSP). PEM and MSP both influenced the development of the most popular Internet email security protocol, which is Secure MIME (S/MIME). This article provides insight into the early history of email security, describes ongoing work to improve email security, and then makes some predictions about the future.

Introduction

This article provides a summary of the early history of email security, describes ongoing work to improve email security, and then makes some predictions about the future.

Privacy Enhanced Mail

The earliest efforts to add security to email took place in the Internet Research Task Force (IRTF). The Privacy and Security Research Group (PSRG) started their work in 1984, and they produced their initial specification in February 1987 [1]. This initial specification was quite difficult to deploy because it depended on manual distribution of symmetric keys. The keys were used to provide message integrity and message confidentiality.

The PSRG continued to make improvements to PEM. In January 1988, support for X.509 version 1 certificates eliminated the need for manual key distribution [2]. In August 1989, greater flexibility in cryptographic algorithm selection was provided [3–5]. In February 1993, services related to key certification were added to the set of specifications [6].

PEM included two key ideas that persist in email security protocols today. First, confidentiality and integrity of the message content was provided by a single-use data encrypting key (DEK). That is, the DEK was generated for the message at hand, and then a fresh one is generated for the next message. Second, the single-use DEK is separately encrypted for each message recipient with a long-lived key. Initially, the long-lived key was distributed manually. Once support for certificates were added to PEM, the public key in the certificate was used as the long-lived key.

Base64 encoding was first specified as part of PEM. Base64 encoding was needed because many email systems did not support the transfer of binary objects. These systems expected email messages to be ASCII text, and Base64 provided a way to transfer the binary ciphertext without changing the email system internals. Today, Base64 encoding is used in many contexts.

PEM was implemented, but it was not widely deployed. PEM was not compatible with Multipurpose Internet Mail Extensions (MIME) [7]. MIME allowed binary attachments to be carried in email messages, and a new email security solution was needed that was compatible with MIME. There is more information about that below.

Secure Data Network System

In 1986, the National Security Agency (NSA) started the Secure Data Network System (SDNS) effort to develop security protocols for the Open System Interconnection (OSI) protocols. The X.400 series of protocol specifications were used to email in the OSI environment, and the SDNS effort produced the Message Security Protocol (MSP) in 1987 [8]. The protocol was completely unclassified, but the cryptography selected by the NSA was not.

MSP used both of the core ideas from PEM; however, the long-lived key was always carried in a certificate. This was not an accident. There was overlap in the teams that developed PEM and MSP. The high-level view of the message format used by MSP is shown in Fig. 1.

MSP always included a digital signature, and message origin authentication was provided by each recipient validating the originator's signature. MSP included a concept that is based on the expected adoption of the X.500 series; the OSI environment was expected to include a global directory system that contained information about all users. MSP assumed that certificates and other digital objects could be fetched from a global directory system; however, the Internet does not have a place to obtain such user-specific information.

MSP included a few features that were absent in PEM, including support for mailing lists, signed receipts from recipients, and label-based access control.

MSP was developed and deployed to about 2 million users as part of the Defense Message System.

Security In X.400 Messaging

The 1988 version of CCITT X.411 Recommendation [9] introduced security features into the X.400 series of electronic message standards. Like PEM and MSP, the encryption and signature were supported. Security features in the mail transfer agents (MTAs) provide protected delivery reporting, and security features in the mail user agent (MUAs) provide selective body part protection, while leaving other body parts unprotected.

Design choices made in X.411 support only key transport algorithms, like RSA, for the management of encryption keys. People that wanted to use key agreement algorithms, like Diffie-Hellman, found the lack of algorithm agility frustrating.

While signatures on individual delivery reports and non-delivery reports are not available in Internet-related message security standards, they can be protected on a hop-by-hop basis by running SMTP [10] and IMAP [11] over a protected transport, such as TLS [12].

The first version of PEM [1] also included provisions for selective message content protection; however, there were user interface challenges to indicate which part of the content was to be protected and which part should remain unprotected. As a result, this capability was dropped in later versions.

Early Versions of Secure MIME

The development of Secure MIME (S/MIME) version 1 and version 2 was driven by RSA Data Security. One of the design goals was to use the same cryptographic primitives as PEM. S/MIME employed MIME conventions to provide encryption and signature of email messages. S/MIME v1 and S/MIME v2 were tightly bound to the RSA algorithm for both key management and digital signature; however, more than one signature on same message content was permitted, which was not supported by PEM or MSP.

In 1998, RSA Data Security turned over change control of the S/MIME specification to the Internet Engineering Task Force (IETF) with the goal of wider adoption [13, 14].

The high-level view of the S/MIME v2 is shown in Fig. 2.

Secure MIME Version 3.0

The IETF published the five RFCs that make up the S/MIME v3.0 specifications in 1999 [15–19]. S/MIME v3.0 offers algorithm agility, but it is backward compatible with S/MIME v2 when the RSA algorithm is employed.

Many of the features from MSP were added to S/MIME v3.0 as options. This was not an accident. The goal was to develop a single email security solution that would meet the needs of industry, government, and military organizations.

The encryption of mail list messages includes a signature from the originator and a second signature (called the outer signature) from the last mail list agent that touched the message. The mail list agent includes the mlExpansionHistory signed attribute to prevent loops when mail lists are misconfigured and to allow different receipt requests for mail list recipients and direct recipients.

S/MIME v3.0 associated security labels with digital signatures, where MSP associated security labels with the encrypted content. This difference allows separate security labels for plaintext and ciphertext. The high-level view of the S/MIME v3.0 is shown in Fig. 3.

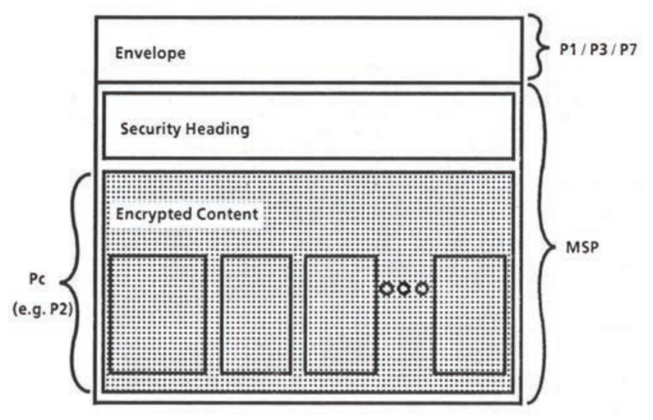
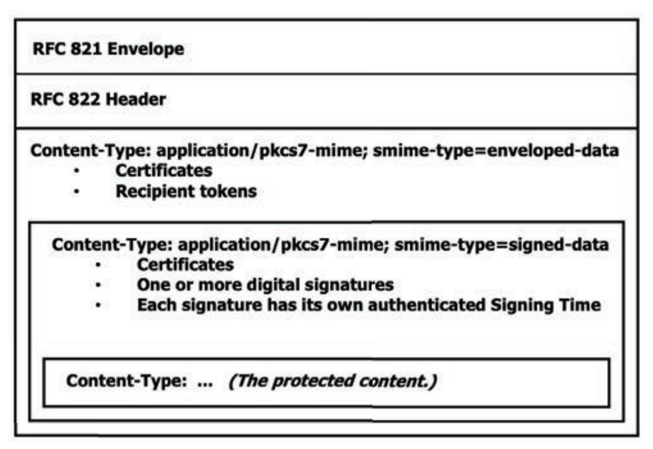


FIGURE 1. Message security protocol.



RFC 821 Envelope

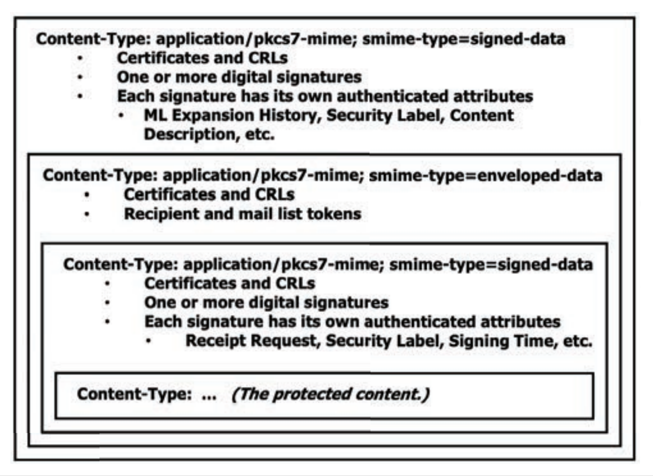
RFC 822 Header

Content-Type: application/pkcs7-mime; smime-type=enveloped-data
- Certificates
- Recipient tokens

Content-Type: application/pkcs7-mime; smime-type=signed-data
- Certificates
- One or more digital signatures
- Each signature has its own authenticated Signing Time

Content-Type: ... *(The protected content.)*

FIGURE 2. S/MIME v2.



Content-Type: application/pkcs7-mime; smime-type=signed-data
- Certificates and CRLs
- One or more digital signatures
- Each signature has its own authenticated attributes
  - ML Expansion History, Security Label, Content Description, etc.

Content-Type: application/pkcs7-mime; smime-type=enveloped-data
- Certificates and CRLs
- Recipient and mail list tokens

Content-Type: application/pkcs7-mime; smime-type=signed-data
- Certificates and CRLs
- One or more digital signatures
- Each signature has its own authenticated attributes
  - Receipt Request, Security Label, Signing Time, etc.

Content-Type: ... *(The protected content.)*

FIGURE 3. S/MIME v3.0.

Internationalized Email Addresses

Two recent IETF publications [20, 21] specify the use of internationalized email addresses in X.509 certificates. With the ability to bind an internationalized email address to a public key, the public keys are used as always to provide signatures on email messages and support encryption of email messages. However, it is taking a very long time for the overall email ecosystem to support internationalized email addresses.

Secure MIME Version 4.0

S/MIME 4.0 [22, 23] includes the usual changes related to cryptographic algorithm aging, and there are two significant changes in S/MIME 4.0, both driven by the "Efail" attack [24].

First, encryption is now performed with an authenticated encryption algorithm. This change ensures message integrity, even if the message content is not signed, and it prevents attacks that manipulate the ciphertext to purposefully inject errors in the underlying plaintext, which is particularly effective when parts of the plaintext are known to the attacker.

Second, implementers are warned about the proper handling of HTML and multipart/mixed in the email message content. To avoid the exfiltration portion of the Efail attack illustrated in Fig. 5, client software needs to protect against maliciously formatted messages by treating the HTML in the email message in a manner similar to the way that a browser handles a web page that references content from multiple origins. Client software protections include:

- Ensure that the message body contains a complete HTML document [25].
- Treat each piece of a multipart/mixed construct as being from different origins.
- Treat each encrypted or signed MIME construct as being from a different origin than the unprotected message content.

Certificates for Secure MIME

The IETF ACME Working Group is specifying easier ways for people to get certificates for use with S/MIME. Earlier work by this group has made it easy for every web server to have a certificate. Hopefully, this new work will have a similar impact on email security.

The CA/Browser Forum is currently developing a set of basic requirements for public certification authorities (CAs) that issue certificates for use with S/MIME [26]. The goal is to provide a high degree of interoperability and hopefully make it much easier to get certificates that support S/MIME. The basic requirements are expected to be finished by the end of 2022.

The emerging requirements describe four certificate profiles and assigns certificate policy identifiers. They are:

- Mailbox-validated: The certificate subject contains a validated email address, but the certificate does not identify the human or organizational affiliation.
- Organization-validated: The certificate includes a validated email address and a validated organizational affiliation, but the certificate does not identify the human.
- Sponsor-validated: The certificate subject contains a validated email address, a validated organizational affiliation, and a validated human identity. A registration authority within the identified organization is likely to validate the identity.
- Individual-validated: The certificate includes a validated email address and a validated human identity, but does not include an organizational affiliation.

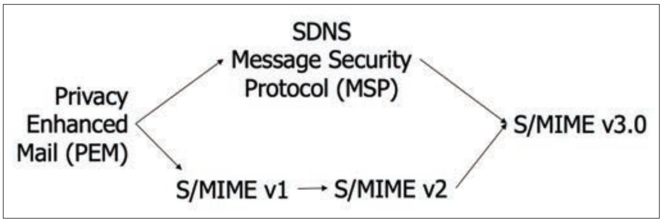
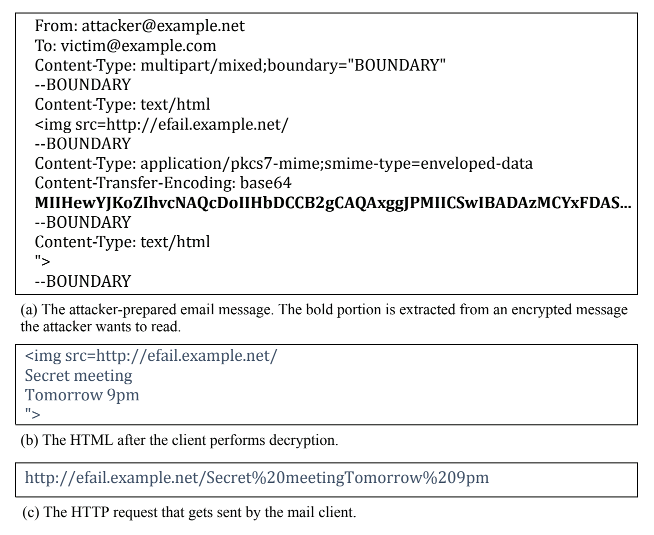


FIGURE 4. Email security protocol influence.



```
From: attacker@example.net
To: victim@example.com
Content-Type: multipart/mixed;boundary="BOUNDARY"
--BOUNDARY
Content-Type: text/html
<img src=http://efail.example.net/
--BOUNDARY
Content-Type: application/pkcs7-mime;smime-type=enveloped-data
Content-Transfer-Encoding: base64
MIIHewYJKoZIhvcNAQcDoIIHbDCCB2gCAQAxggJPMIICSwIBADAzMCYxFDAS...
--BOUNDARY
Content-Type: text/html
">
--BOUNDARY
```

(a) The attacker-prepared email message. The bold portion is extracted from an encrypted message the attacker wants to read.

```
<img src=http://efail.example.net/
Secret meeting
Tomorrow 9pm
">
```

(b) The HTML after the client performs decryption.

```
http://efail.example.net/Secret%20meetingTomorrow%209pm
```

(c) The HTTP request that gets sent by the mail client.

FIGURE 5. Sample Efail attack.

Once this effort is finished, the expectation is that all email users will be able to get certificates for use with S/MIME with minimal hassle and little expense.

Header Protection

The IETF LAMPS Working Group is currently working on a specification to improve the conventions used for optional protection of email message headers, especially the subject line of the message. Today, most client software encrypts and signs only the body of the message, which leaves the subject line of the message and other headers open to manipulation by attackers.

Starting with S/MIME 3.1 [27], an entire email message, including its headers, could be protected and carried inside the email message. This is often called a "wrapped message," and it leads to some confusion because some client software presented the wrapped message in the same way as a forwarded message.

To avoid this confusion, another form of header protection is under development, called "injected headers," where the subject line of the message and other headers are simply repeated at the beginning of the message. This approach lets the user compare the unprotected and protected headers. Eventually, client software might perform this comparison automatically, and then warn the user when they do not match.

Quantum Safe Cryptography

The development of a large-scale quantum computer would pose a serious challenge for the cryptographic algorithms that are widely deployed today. It is an open question whether or not it is feasible to build a large-scale quantum computer, and if so, when that might happen. However, if such a quantum computer is invented, the messages protected with S/MIME would become vulnerable.

To protect against potential invention of a large-scale quantum computer, the National Institute of Science and Technology (NIST) is developing standards for quantum-safe cryptographic algorithms [28]. The to-be-standard algorithms have been chosen, but the NIST standards will not be finalized until 2024. The IETF LAMPS Working Group is specifying the conventions for using these new algorithms in certificates and S/MIME. This may lead to yet another version of the S/MIME standard.

Conclusion

It is becoming easier to get certificates that work with S/MIME. The recent work of the IETF LAMPS Working Group provides an opportunity to use internationalized email addresses. Hopefully, the work of the IETF ACME Working Group and the CA/Browser Forum will make it much easier for all users to get certificates that contain their email addresses.

Support for internationalized email address throughout the Internet is slowly being rolled out, but full support will take many more years.

The ongoing work will reduce the opportunities for malicious actors to tamper with any portion of the email message that users expect to be secure, including the message subject line.

New cryptographic algorithms are coming. The specifications will be updated, and then client software will need to be updated to use them. This transition will take many years.

References

[1] J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I — Message Encipherment and Authentication Procedures,", IETF RFC 989, Feb. 1987; https://www.rfc-editor.org/info/rfc989. DOI 10.17487/RFC0989.

[2] J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I — Message Encipherment and Authentication Procedures," IETF RFC 1040, Jan. 1988; https://www.rfc-editor.org/info/rfc1040. DOI 10.17487/RFC1040.

[3] J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part I — Message Encipherment and Authentication Procedures," IETF RFC 1113, Aug. 1989; https://www.rfc-editor.org/info/rfc1113. DOI 10.17487/RFC1113.

[4] S. Kent and J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part II — Certificate-Based Key Management," IETF RFC 1114, Aug. 1989; https://www.rfc-editor.org/info/rfc1114. DOI 10.17487/RFC1114.

[5] J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part III — Algorithms, Modes, and Identifiers," IETF RFC 1115, Aug. 1989; https://www.rfc-editor.org/info/rfc1115.

[6] B. Kaliski, "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services," IETF RFC 1424, Feb. 1993; https://www.rfc-editor.org/info/rfc1424. DOI 10.17487/RFC1424.

[7] N. Borenstein and N. Freed, "MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies," IETF RFC 1341, June 1992; https://www.rfc-editor.org/info/rfc1341. DOI 10.17487/RFC1341.

[8] C. Dinkel, Ed. "SDNS Message Security Protocol, Specification SDN.701, Revision 1.5." in Secure Data Network System (SDNS) Network, Transport, and Message Security Protocols, NISTIR 90-4250, NIST, 1990.

[9] CCITT Rec. X.411, "Message Handling Systems (MHS) — Message Transfer System: Abstract Service Definition and Procedures," Nov. 1988; https://www.itu.int/rec/T-REC-X.411-198811-S.

[10] J. Klensin, "Simple Mail Transfer Protocol," IETF RFC 5321, Oct. 2008; https://www.rfc-editor.org/info/rfc5321. DOI 10.17487/RFC5321.

[11] M. Crispin, "Internet Message Access Protocol — Version 4rev1," IETF RFC 3501, Mar. 2003; https://www.rfc-editor.org/info/rfc3501. DOI 10.17487/RFC3501

[12] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF RFC 8446, Aug. 2018; https://www.rfc-editor.org/info/rfc8446. DOI 10.17487/RFC8446.

[13] S. Dusse *et al.*, "S/MIME Version 2 Message Specification," IETF RFC 2311, Mar. 1998; https://www.rfc-editor.org/info/rfc2311. DOI 10.17487/RFC2311.

[14] S. Dusse *et al.*, "S/MIME Version 2 Certificate Handling," IETF RFC 2312. DOI 10.17487/RFC2312, Mar. 1998; https://www.rfc-editor.org/info/rfc2312.

[15] R. Housley, "Cryptographic Message Syntax," IETF RFC 2630, June 1999; https://www.rfc-editor.org/info/rfc2630. DOI 10.17487/RFC2630.

[16] E. Rescorla, "Diffie-Hellman Key Agreement Method," IETF RFC 2631, June 1999; https://www.rfc-editor.org/info/rfc2631. DOI 10.17487/RFC2631.

[17] B. Ramsdell, Ed., "S/MIME Version 3 Certificate Handling," IETF RFC 2632ME Version 3 Message Specification," IETF RFC 2633, June 1999; https://www.rfc-editor.org/info/rfc2633. DOI 10.17487/RFC2633.

[19] P. Hoffman, Ed., "Enhanced Security Services for S/MIME," IETF RFC 2634, June 1999; https://www.rfc-editor.org/info/rfc2634. DOI 10.17487/RFC2634.

[20] A. Melnikov and W. Chuang, Eds., "Internationalized Email Addresses in X.509 Certificates," IETF RFC 8398, May 2018; https://www.rfc-editor.org/info/rfc8398. DOI 10.17487/RFC8398.

[21] R. Housley, "Internationalization Updates to RFC 5280," IETF RFC 8399, May

2018; https://www.rfc-editor.org/info/rfc8399. DOI 10.17487/RFC8399.

[22] J. Schaad, B. Ramsdell, and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Certificate Handling," IETF RFC 8550, Apr. 2019; https://www.rfc-editor.org/info/rfc8550. DOI 10.17487/RFC8550.

[23] J. Schaad, B. Ramsdell, and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification," IETF RFC 8551, Apr. 2019; https://www.rfc-editor.org/info/rfc8551. DOI 10.17487/RFC8551.

[24] D. Poddebniak *et al.*, "Efail: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels," UsenixSecurity 2018, Aug. 2018; https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-poddebniak.pdf.

[25] T. Berners-Lee and D. Connolly, "Hypertext Markup Language — 2.0," IETF RFC 1866, Nov. 1995; https://www.rfc-editor.org/info/rfc1866. DOI 10.17487/RFC1866.

[26] https://cabforum.org/working-groups/smime-certificate-wg/

[27] B. Ramsdell, Ed., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification," IETF RFC 3851, July 2004; https://www.rfc-editor.org/info/rfc3851. DOI 10.17487/RFC3851.

[28] https://csrc.nist.gov/News/2022/pqc-candidates-to-be-standardized-and-round-4

Biography

Russell Housley [M] (housley@vigilsec.com) is an expert in security protocols. He authored many Internet standards, including the Cryptographic Message Syntax (RFC 5652) and the Internet X.509 Certificate Profile (RFC 5280). He served as Chair of IETF from 2007 to 2013. He served on the Internet Architecture Board (IAB) from 2007 to 2017, and Chair of the IAB from 2013 to 2015. He was IETF Security Area Director from 2003 to 2007.