End-to-End Header Protection in S/MIME and PGP mail

Lijun Liao and Jörg Schwenk
Horst-Görtz Institute for IT-Security, Ruhr-University of Bochum
{lijun.liao,joerg.schwenk}@nds.rub.de

1. Introduction

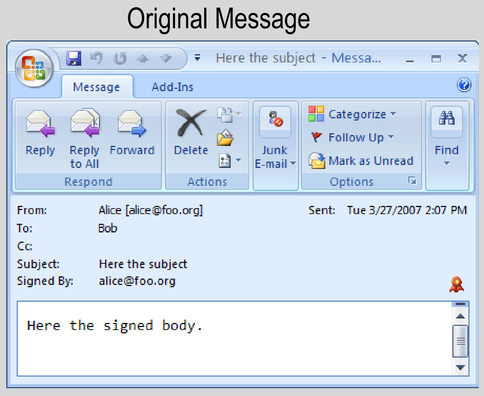
S/MIME (Secure MIME) and PGP mail are the most popular mechanisms for signing emails. In both mechanisms only the email content is protected, but the email headers are not authenticated. DKIM (DomainKeys Identified Mail) protects specified headers, but only between the sending server and the receiver. This leads to possible impersonation attacks, and encourages spam and phishing activities. To avoid such attacks we extend S/MIME and PGP mail to support end-to-end header protection. Our extension is fully compatible with the prior versions, and can be implemented easily.

2. Problems

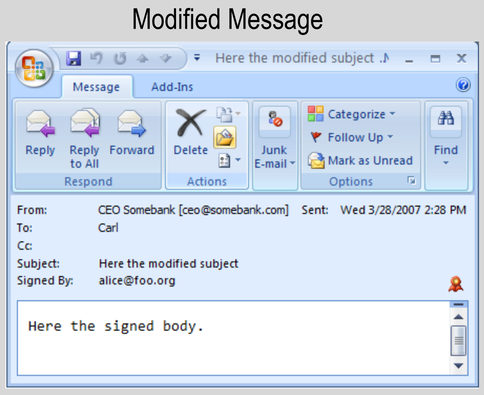
- In signed emails, only the email body is protected by the signature
- Email headers like `From`, `To`, and `Subject` are not protected by the signature
- The `From` header is only secure if the email client checks that the `From` address matches
  - the Internet mail address in the subject (in S/MIME), or
  - the user ID (in PGP mail)

  of the signer's certificate. In fact, the most popular email client Microsoft Outlook does not check this

Original Message



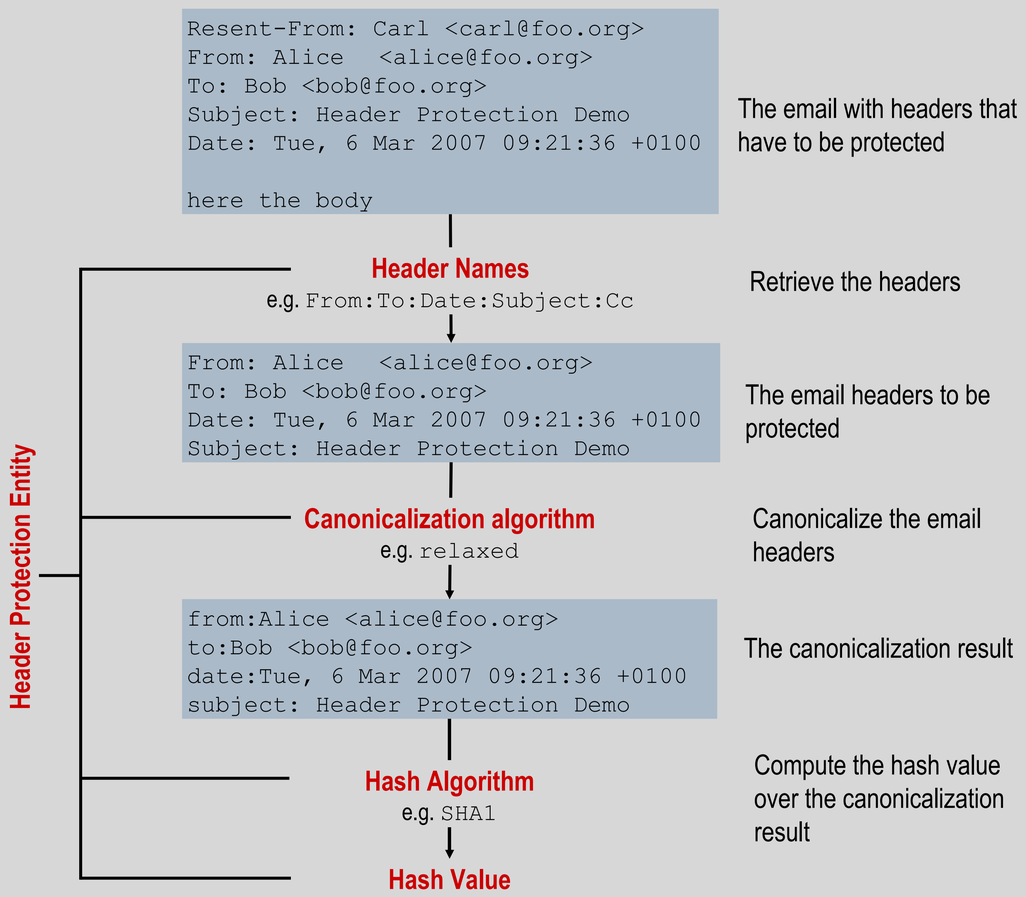
Modified Message



Modified headers (`From`, `To`, `Date`, and `Subject`), but still valid signature in Outlook

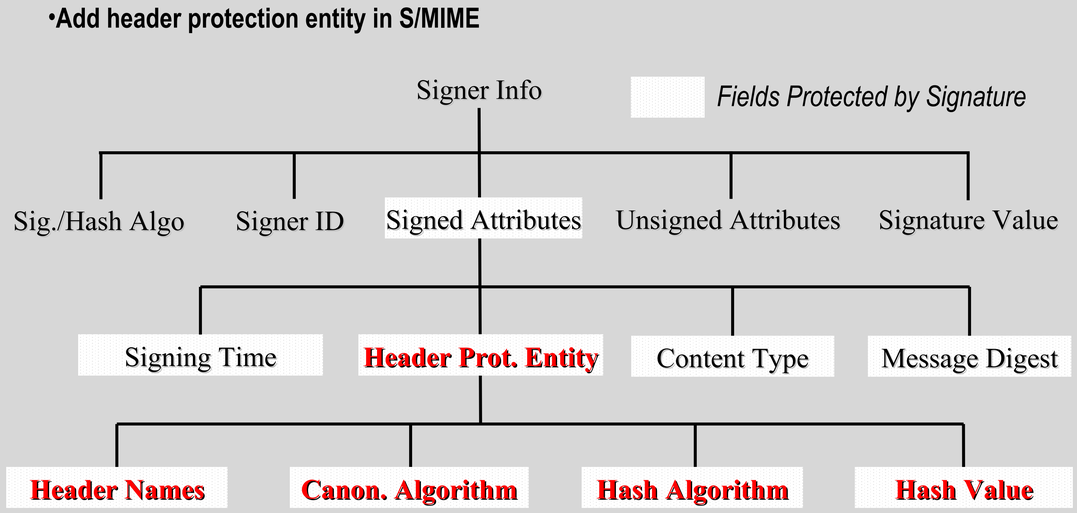
3. Materials and Methods

- **Header Protection Entity**

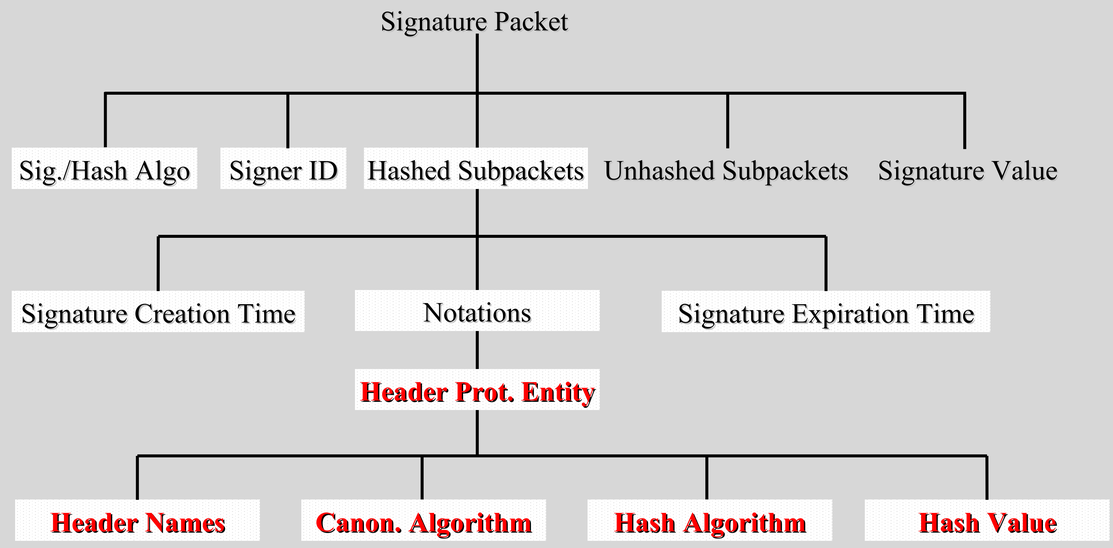


Process of Computing an Header Protection Entity

- **Add header protection entity in S/MIME**



- **Add header protection entity in PGP mail**



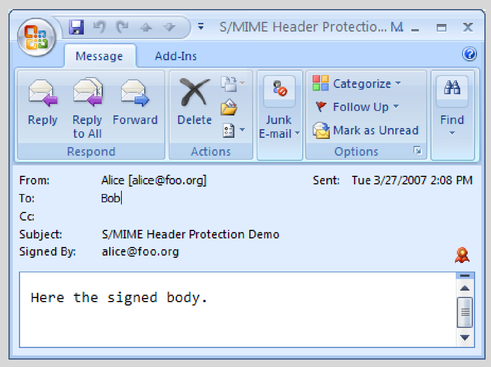
4. Results

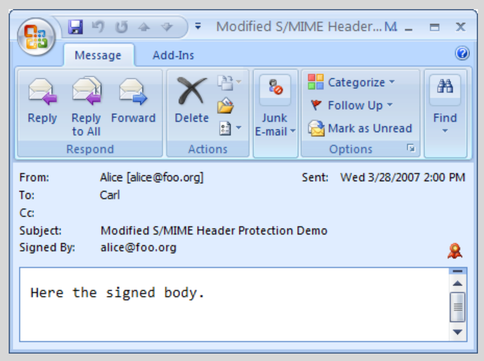
- S/MIME and PGP mail with our extension protect the entire message, i.e. the email headers and email body, between the sender and the receiver
- Email clients that do not know our extension can verify the signature as usual, but cannot detect any modifications of the headers
- Since the used cryptographic functions are available in S/MIME or PGP capable clients, our extension can be implemented easily

Original S/MIME Message

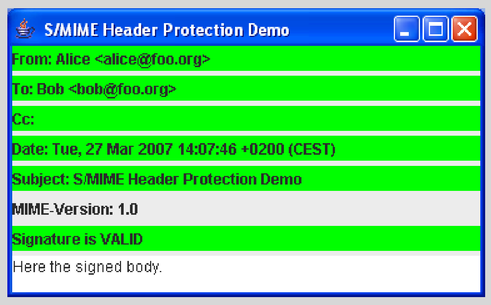
S/MIME Message with Modified Headers

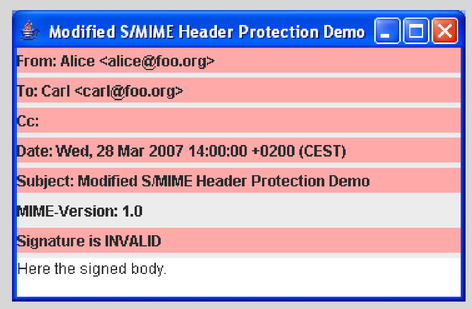
Outlook 2007





Our Prototype API





S/MIME Message (with protected headers `From`, `To`, `Cc`, `Subject`, `Date`) in Clients

5. Conclusion

- Modifications of headers can be detected by our approach
- With some reasonable assumptions, our approach provides efficient methods to struggle with spam
- S/MIME is widely accepted, thus implemented header protection is of great importance
- As our future work, we will implement extensions for the popular email clients to support header protection

6. Bibliography

- B. Ramsdell (Editor), Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1, IETF RFC 3851, July 2004
- J. Callas et. al. OpenPGP Message Format, IETF RFC 2440, Nov. 1998
- M. Elkins et. al. MIME Security with OpenPGP, IETF RFC 3156, Aug. 2001
- E. Allman et. al. DomainKeys Identified Mail (DKIM) Signatures, IETF Internet-Draft, Feb. 2007