



Message Security Protocols

William P. Flinn

Colorado Technical University

CS-653, Summer, 2005



Overview

- Securing messages
- Privacy enhanced mail (PEM)
- MIME object security services (MOSS)
- Pretty Good Privacy (PGP)
- Secure MIME (S/MIME)
- Summary



Securing Messages

- Use a secure transfer protocol to carry the unsecured bits
 - Services provided at the application layer
 - Such as SSH or other methods
- Use an insecure transfer protocol, but secure the bits
 - Encryption



Privacy Enhanced Mail (PEM)

- Early effort by the IRTF Privacy and Security Research Group
- Later by the IETF
- Never succeeded in commercial deployment
 - Limited to 7-bit ASCII
 - Strict use of hierarchy of CAs that serve as a PKI for PEM
- Introduced the use of digital envelopes and base-64 encoding scheme



MIME Object Security Services (MOSS)

- RFC-1848
- Attempted to overcome the limitations of PEM
 - Namely the incompatibility with MIME and strict PKI requirements



Pretty Good Privacy (PGP)

- PGP is a software package – not a protocol
- Developed by Richard Zimmermann in early 1990s
- Used MD5, IDEA and RSA as building blocks
- PGP 9.0 Beta now available for 30 day trial

<http://www.pgpi.org/>



Pretty Good Privacy (PGP)

- Legal problems:
 - PGP software uses RSA algorithm – protected by U.S. patent
 - U.S. Government export controls violated when PGP software made available as freeware
- After government dropped case, Zimmermann founded Pretty Good Privacy, Inc.



Pretty Good Privacy (PGP)

- The “nuts and bolts”:
 - Uses public and private keys
 - Public key so your friends can encrypt their messages to you.
 - Private key so you can decrypt your friends’ messages
 - Public key can be stored on a certificate server where people can pick it up.
 - Public key can also be sent in an email



Pretty Good Privacy (PGP)

- PGP uses both symmetrical (IDEA) and asymmetrical (public/private key pair)
- Uses a session key to encrypt the bulk of the message
 - IDEA, symmetrical encryption
- Uses public key to encrypt the session key and adds it to the encrypted data.



Pretty Good Privacy (PGP)

- Stores public and private keys in files called “keyrings”
 - Pubring.pgp
 - Secring.pgp



Secure Multipurpose Internet Mail Extensions (S/MIME)

- Specification as opposed to being a product like PGP
- Designed to add security to email messages that use MIME message formats
- User agents must support S/MIME
- Built on top of public key cryptography standard and uses ASN.1 specifications
- Relies on public key certificates issued by CAs



Secure Multipurpose Internet Mail Extensions (S/MIME)

○ Versions:

- S/MIME 1 – Published in 1995 by RSA Security, Inc.
- S/MIME 2 – Specified in RFC 2311 and RFC 2312 in March, 1998
- S/MIME 3 – IETF S/MIME Mail Security WG in June, 1999. Specified in RFC 2633



Summary

- PEM and MOSS older, limited efforts
- PGP and S/MIME recognized as “the way to go” for email and messaging security
- PGP is a software package that can be installed separately
- S/MIME is a specification and requires user agents to support S/MIME