E-mail Security

BİL 448/548
Internet Security Protocols
Ali Aydın Selçuk

Security Services for E-mail

- privacy
- authentication
- integrity
- non-repudiation
- anonymity
- proof of submission
- proof of delivery
- message flow confidentiality, etc.

Key Management

- A per-message symmetric key is used for message encryption,
- which is conveyed in the mail, encrypted under a long-term key (typically a public key)
- Long-term keys can be established,
  - offline
  - online, with help from a trusted third party
  - online, through a webpage (for public keys)

Multiple Recipients

- Message key will be encrypted under each recipients long term key in the message header.
  - Bob's ID, $K_{Bob}\{S\}$
  - Carol's ID, $K_{Carol}\{S\}$
  - Ted's ID, $K_{Ted}\{S\}$
  - S{m}
- E.g.:

```
To: Bob, Carol, Ted
From: Alice
Key-info: Bob-4276724736874376
Key-info: Carol-78657438676783457
Key-info: Ted-12873486743009
Msg-info: UHGuiy77t65fhj87oi.....
```

Text Format Issues

- Mail gateways/forwarders may modify the format of the message (wrapping long lines, end-of-line character, high order bits, etc.), causing the integrity check to fail
- Encode messages in a format supported by all mailers; 6-bit representation, no long lines, etc. (Base64 encoding). (*)

(*) Tutorial on character coding: http://www.cs.tut.fi/~jkorpela/chars.html

Text Format Issues (cont'd)

- Problem: Authentication-only (not encrypted) mails should be readable by non-supportive clients.
- Two options:
  - Sign without encoding (*)
    (subject to corruption by mail routers)
  - Encode & sign
    (may not be readable at the other end)

(*) First option is popular.

PEM & S/MIME

- Privacy Enhanced Mail (PEM)
  - Developed by IETF, to add encryption, source authentication & integrity protection to e-mail
  - Allows both public & secret long-term keys
    Message key is always symmetric
  - Specifies a detailed certification hierarchy
- Secure/MIME (S/MIME)
  - PEM never took off; CA hierarchy difficult to realize
  - S/MIME: PEM design incorporated into MIME

PEM Key Exchange & Encryption

- "Interchange keys": Users' long-term PEM keys
  - public (a detailed PKI is defined)
  - secret (pre-shared symmetric keys)
- Encryption
  - A symmetric per-message key is sent encrypted under the interchange key.
  - The message is encrypted under the per-message key (typically with DES in CBC mode)
- Authentication
  - Message is authenticated by a "MIC"
    (Q: Any authentication for the per-message key?)

PEM Certificate Hierarchy

- The root CA: “Internet Policy Registration Authority” (IPRA)
- “Policy Certification Authorities”: Second-level, CA-certifying CAs, each with a different policy:
  - High Assurance (HA): super-secure
    - implemented on secure platforms
    - regulates that the child CAs (also HACAs) enforce the same rules
  - Discretionary Assurance (DA): secure
    - requires that the child CAs own their names
  - No Assurance (NA): no constraints
    - can be used to certify Internet personas (pseudonyms)
- Lower-level CAs, certifying individuals or other CAs

S/MIME vs. PEM

- Incorporated into MIME; no other encoding
- Any sequence of sign & encrypt is supported (each as a recursive MIME encapsulation)
- Has more options than PEM
- ASN.1 header encoding
- No prescribed certification hierarchy
- Has a good prospect of deployment for commercial & organizational usage

Pretty Good Privacy (PGP)

- Popular mail & file encryption tool
- Developed by Phil Zimmermann, 1991
- Originally based on RSA, IDEA, MD5 (later DSS, ElGamal, 3DES, AES, SHA1)
- Many different versions have emerged (from PGP, from GNU (GPG), from IETF (Open PGP))

PGP Operation

- All long-term user keys are public
- Signature:

  Message & timestamp are hashed (MD5 or SHA1) and signed (RSA or DSS)
- Compression before encryption (ZIP)
- Encryption:
  - Message is encrypted with a per-message symmetric key; typically in CFB mode. (Why?)
  - That key is encrypted with the recipient’s public key (RSA or DH (ElGamal)).
- Base64 (6-bit) encoding

PGP Trust Model & Key Management

- Any user can certify any other (anarchy model)
- Each user decides whom to trust and how much
- "Key Ring": Data structure to store public keys held by a user, with their levels of trust
- Public keys can be obtained,
  - offline (in person, over the phone, etc.)
  - through personal webpages
  - through a trusted friend ("web of trust")
  - through a trusted repository (e.g., keyserver.pgp.com)

DKIM – Domain Keys Identified Mail

- An effort to stop spam with forged domain addresses (e.g. phishing attacks).
- Standardized by RFC 4871; supported by Yahoo, Gmail, FastMail etc.
- Each domain has an email signature key. Public keys will be retrieved over DNS.
- If signature verification fails, mail will be dropped.

DKIM

- Once deployed, it will significantly limit phishing attacks with forged domain addresses.
- Deployment is increasing rapidly.
- Example: Gmail's collaboration with PayPal & eBay