Electronic Mail Security

General Principles

Security Services for Electronic Mail

- privacy
- source authentication
- message integrity
- non-repudiation
- proof of submission
- proof of delivery
- message flow confidentiality
- anonymity
- containment
- audit
- accountancy
- self destruct
- message sequence integrity

Privacy

- protection against eavesdropping
- may conflict with organisational security monitoring
- For a message sent to multiple recipients

  - choose random key S

  - encrypt message once with S

  - send S encrypted under recipient’s public key in each message

Message Integrity and Source Authentication – Public Key

- To sign message to multiple recipients

  - form Message Digest of message

  - sign digest with private key

  - send to all recipients with public key and certificate chain if necessary
- Message integrity provided by same method

Message Integrity and Source Authentication – Private Key

- To sign a message to single recipient who shares a secret with sender

  - compute CBC residue to form MAC, or

  - form message digest of secret concatenated with message, or

  - encrypt message digest of message with secret key
- Use last message for multiple recipients

Non-Repudiation

- Provided simply in public key cryptography by private key signature
- May use private key cryptography with aif of third party or notary

  - A proves with secret shared with notary N that it has created message

  - N calculates a seal with its own secret shared with nobody

  - N signs seal with secret shared with B

Message Flow Confidentiality

- Enclose message in encrypted message to third party for forwarding

- use service which sends encrypted dummy messages to several recipients

- Use several intermediaries in nested encrypted chain

Other Security Matters (I)

- Anonymity – recipient cannot establish sender’s identity – e.g. by forwarding through third party
- Containment – security regions established in network which receive mail of appropriate security class
- Audit – ability for network to record all events od relevance to security

Other Security Matters (II)

- Accounting – maintenance of usage statistics
- Self destruct – option to allow message to be destroyed after delivery – i.e. message cannot be forwarded or stored
- message sequence integrity – integrity for entire sequence