Email Security

Email Security

1. email is one of the most widely used and regarded network services
2. currently message contents are not secure
    a. may be inspected either in transit
    b. or by suitably privileged users on destination system

Email Security Enhancements

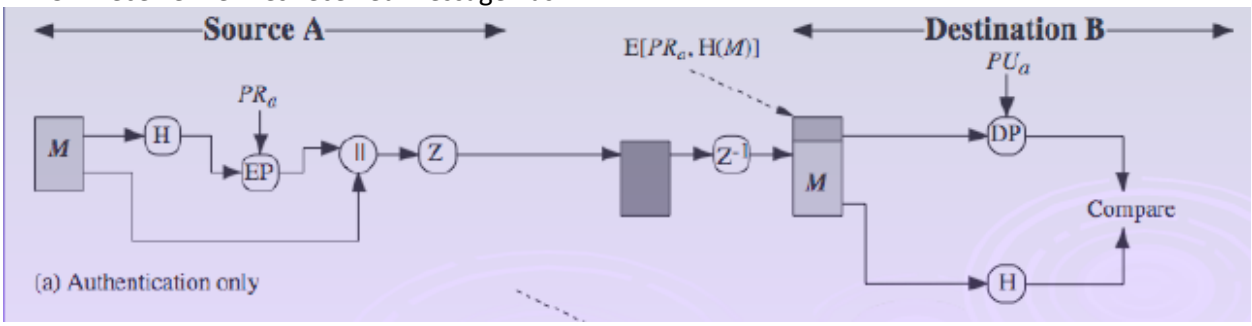
1. Confidentiality : protection from disclosure
2. Authentication : of sender of message
3. message integrity : protection from modification
4. non-repudiation of origin : protection from denial by sender

Pretty Good Privacy (PGP)

1. widely used de facto secure email
2. developed by Phil Zimmermann
3. selected best available crypto algs to use
4. integrated into a single program

PGP Operation – Authentication

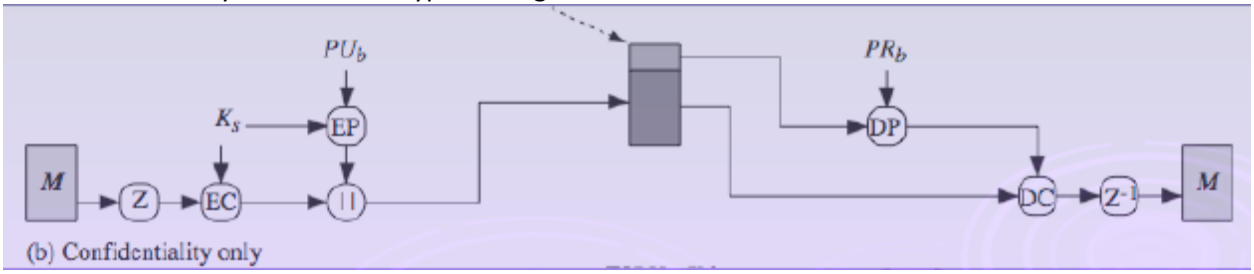
1. sender creates message
2. make SHA-1 160-bit hash of message
3. attached RSA signed hash to message
4. receiver decrypts & recovers hash code
5. receiver verifies received message hash



PGP Operation – Confidentiality

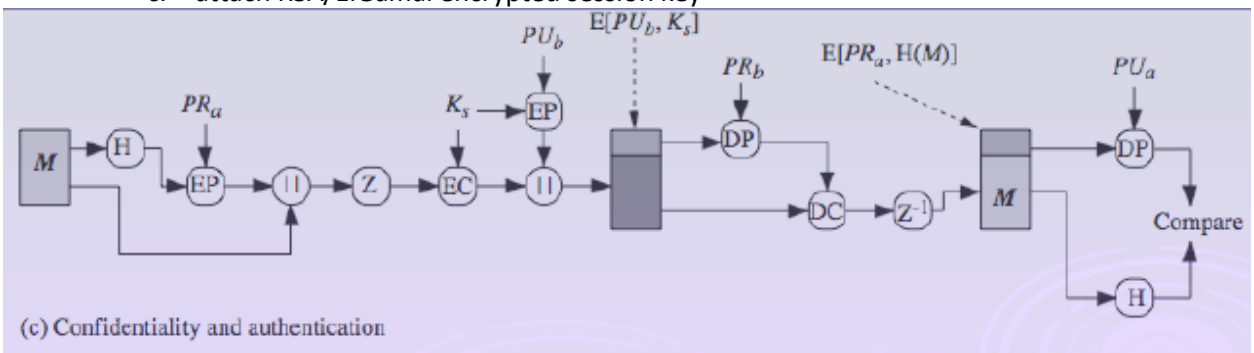
1. sender forms 128-bit random session key
2. encrypts message with session key
3. attaches session key encrypted with RSA

4. receiver decrypts & recovers session key
5. session key is used to decrypt message



PGP Operation – Confidentiality & Authentication

1. can use both services on same message
    a. create signature & attach to message
    b. encrypt both message & signature
    c. attach RSA/ElGamal encrypted session key



PGP Operation – Email Compatibility

1. when using PGP will have binary data to send (encrypted message etc.)
2. however email was designed only for text
3. hence PGP must encode raw binary data into printable ASCII characters
4. uses radix-64 algorithm (aka "ASCII Armour")
    a. maps 3 bytes to 4 printable chars (it's the Base64 of MIME)
    b. also appends a 24-bit CRC
5. PGP also segments messages if too big

S/MIME (Secure/Multipurpose Internet Mail Extensions)

1. security enhancement to MIME email
2. original Internet RFC822 email was text only
3. MIME provided support for varying content types and multi-part messages
4. with encoding of binary data to textual form
5. S/MIME added security enhancements
6. have S/MIME support in many mail agents
    a. eg MS Outlook, Mozilla, Mac Mail etc

S/MIME Functions

1. enveloped data : encrypted content and associated keys
2. signed data : encoded message + signed digest
3. clear-signed data : cleartext message + encoded signed digest
4. signed & enveloped data : nesting of signed & encrypted entities

S/MIME Cryptographic Algorithms

1. digital signatures: DSS & RSA
2. hash functions: SHA-1 & MD5
3. session key encryption: ElGamal & RSA
4. message encryption: AES, Triple-DES, RC2/40 and others
5. MAC: HMAC with SHA-1 have process to decide which algs to use

S/MIME Messages

1. S/MIME secures a MIME entity with a signature, encryption, or both
2. forming a MIME wrapped PKCS object
3. have a range of content-types:
    a. enveloped data
    b. signed data
    c. clear-signed data
    d. registration request
    e. certificate only message

S/MIME Certificate Processing

1. S/MIME uses X.509 v3 certificates
2. managed using a hybrid of a strict X.509 CA hierarchy & PGP's web of trust
3. each client has a list of trusted CA's certs
4. and own public/private key pairs & certs
5. certificates must be signed by trusted CA's

Certificate Authorities

1. have several well-known CA's
2. Verisign one of most widely used
3. Verisign issues several types of Digital IDs
4. increasing levels of checks & hence trust

    Class Identity Checks Usage

    a. name/email check web browsing/email
    b. + enroll/addr check email, subs, s/w validate
    c. + ID documents e-banking/service access

S/MIME Enhanced Security Services

1. 3 proposed enhanced security services:
    a. signed receipts
    b. security labels
2. secure mailing lists