CN414
Computer Network Security

Week 7:- Pretty Good Privacy

By Dr. Piya Techateerawat

Lecture slides by Lawrie Brown Chapter 15

Email Security

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

Email Security Enhancements

- confidentiality
  - protection from disclosure
- authentication
  - of sender of message
- message integrity
  - protection from modification
- non-repudiation of origin
  - protection from denial by sender

Pretty Good Privacy (PGP)

- Open source, freely available software package for secure e-mail
- de facto standard for secure email
- developed by Phil Zimmermann
- selected best available crypto algs. to use
- Runs on a variety of platforms like Unix, PC, Macintosh and other systems
- originally free (now also have commercial versions available)

PGP Operation – Authentication

1. sender creates message
2. Generates a digital signature for the message
3. use SHA-1 to generate 160-bit hash of message
4. signed hash with RSA using sender's private key, and is attached to the message
5. receiver uses RSA with sender's public key to decrypt and recover hash code
6. receiver verifies received message using hash of it and compares with decrypted hash code

PGP Operation – Confidentiality

1. sender generates a message and encrypts it.
2. Generates a128-bit random number as the session key
3. Encrypts the message using CAST-128/IDEA/ 3DES in CBC mode with the session key
4. session key encrypted using RSA with recipient's public key and attached to the msg.
5. receiver uses RSA with private key to decrypt and recover session key
6. The session key is used to decrypt message

PGP Operation – Confidentiality & Authentication

- can use both services on the same message
  - create signature & attach it to the message
  - encrypt both message & signature
  - attach RSA/ElGamal encrypted session key

  This sequence is preferred because

  --one can store the plaintext message/file and its signature

  --no need to decrypt the message/file again and again

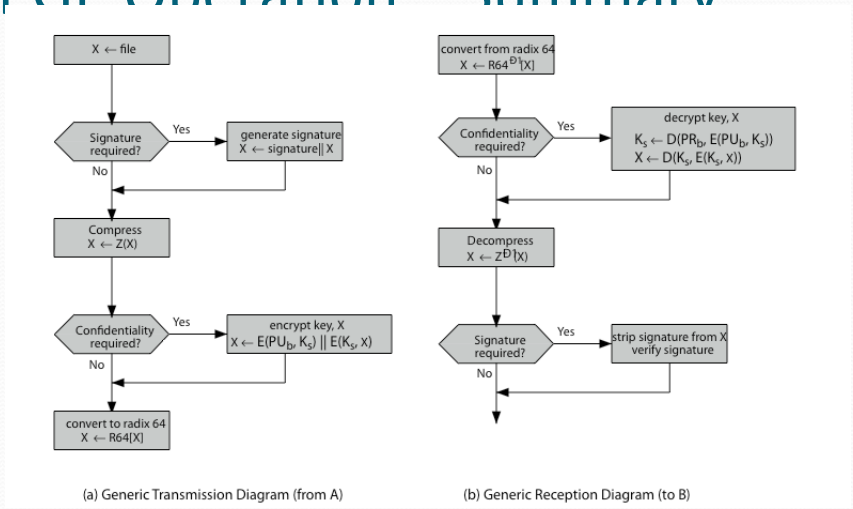
PGP Operation – Compression

- PGP compresses messages to save space for e-mail transmission and storage
- by default PGP compresses message after signing but before encrypting
  - so can store uncompressed message & signature for later verification
  - Encryption after compression strengthens security (because compression has less redundancy)
- uses ZIP compression algorithm

PGP Operation – Email Compatibility

- when using PGP, will have binary data (8-bit octets) to send (encrypted message, etc.)
- however email was designed only for text
- hence PGP must encode raw binary data into printable ASCII characters
- uses radix-64 algorithm
  - maps 3 bytes to 4 printable chars
  - also appends a CRC
- PGP also segments messages if too big (maximum length 50,000 octets)

PGP Operation – Summary



(a) Generic Transmission Diagram (from A)

(b) Generic Reception Diagram (to B)

PGP Session Keys

- need a session key for each message
  - of varying sizes: 56-bit DES, 128-bit CAST or IDEA, 168-bit Triple-DES
- uses random inputs taken from

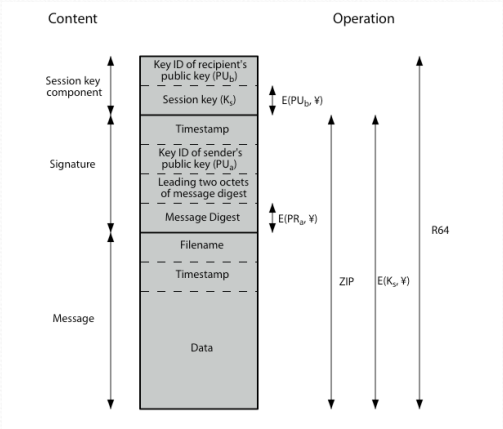
  -actual keys hit

  -keystroke timing of a user

PGP Public & Private Keys

- since many public/private keys may be in use, need to identify which is actually used to encrypt session key in a message
  - could send full public-key with every message
  - but this is inefficient
- rather use a key identifier based on key
  - is least significant 64-bits of the key
  - will very likely be unique
- also use key ID in signatures

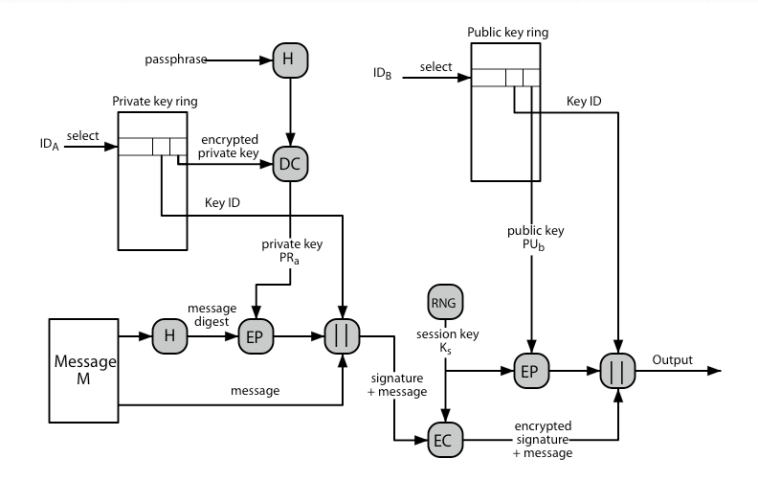
PGP Message Format



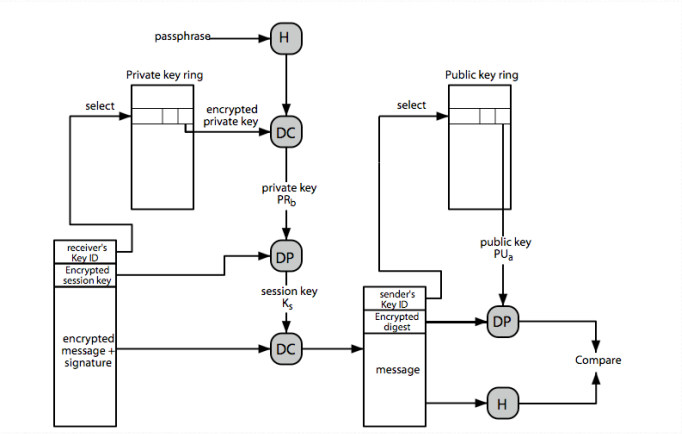
PGP Key Rings

- each PGP user has a pair of keyrings:
  - public-key ring contains all the public-keys of other PGP users known to this user, indexed by key ID
  - private-key ring contains the public/private key pair(s) for this user, indexed by key ID & encrypted keyed from a hashed passphrase
- security of private keys thus depends on the pass-phrase security

PGP Message Generation



PGP Message Reception



Summary

- have considered:
  - secure email
  - PGP

Reference

- Lecture slides by Lawrie Brown Chapter 15


Q & A