SNS COLLEGE OF TECHNOLOGY

Coimbatore-35
An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A+' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

TOPIC : EMAIL SECURITY

THREATS

- Threats to the security of e-mail itself
  - Loss of confidentiality
    - E-mails are sent in clear over open networks
    - E-mails stored on potentially insecure clients and mail servers
  - Loss of integrity
    - No integrity protection on e-mails; body can be altered in transit or on mail server
  - Lack of data origin authentication
  - Lack of non-repudiation
  - Lack of notification of receipt

THREATS ENABLED BY E-MAIL

- Disclosure of sensitive information
- Exposure of systems to malicious code
- Denial-of-Service (DoS)
- Unauthorized accesses etc.

WHAT ARE THE OPTIONS

- Secure the server to client connections (easy thing first)
  - POP, IMAP over ssh, SSL
  - https access to webmail
  - Very easy to configure
  - Protection against insecure wireless access
- Secure the end-to-end email delivery
  - The PGPs of the world
  - Still need to get the other party to be PGP aware
  - Practical in an enterprise intra-network environment

EMAIL BASED ATTACKS

- Active content attack
  - Clean up at the server (AV, Defang)
- Buffer over-flow attack
  - Fix the code
- Shell script attack
  - Scan before send to the shell
- Trojan Horse Attack
  - Use “do not automatically use the macro” option
- Web bugs (for tracking)
  - Mangle the image at the mail server

EMAIL SPAM

- Cost to exceed $10 billion
- SPAM filtering
  - Content based – required hits
  - White list
  - Black list
  - Defang MIME

PGP

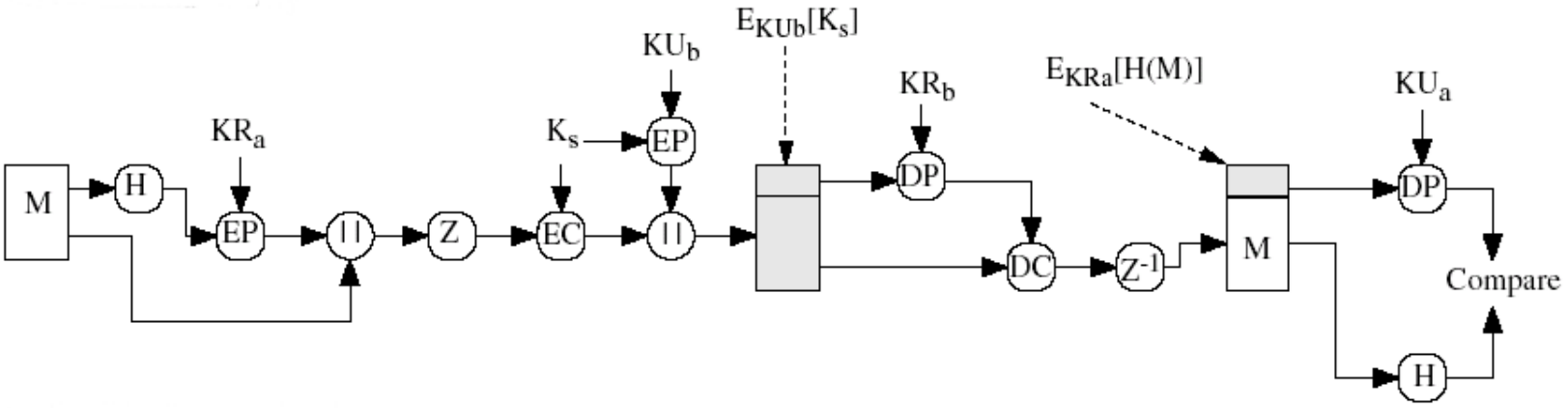
- PGP="Pretty Good Privacy"
- Functionality
  - Encryption for confidentiality.
  - Signature for non-repudiation/authenticity.
- Sign before encrypt, so signatures on unencrypted data - can be detached and stored separately.
- PGP-processed data is `base64` encoded

PGP ALGORITHMS

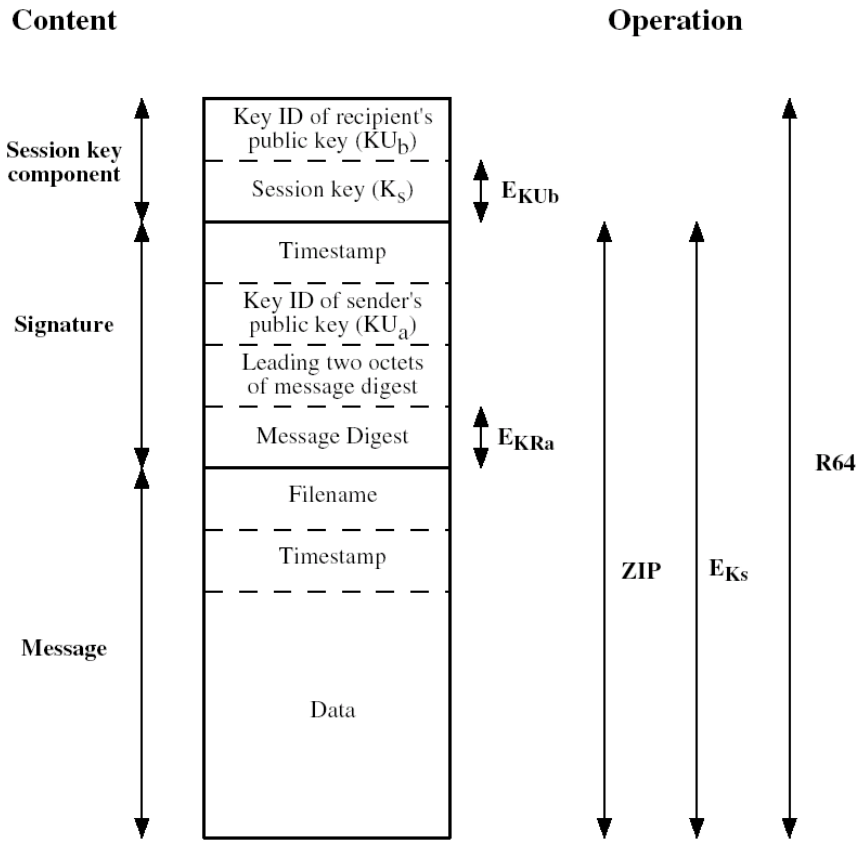
Broad range of algorithms supported:

- Symmetric encryption:
  - DES, 3DES, AES and others.
- Public key encryption of session keys:
  - RSA or ElGamal.
- Hashing:
  - SHA-1, MD-5 and others.
- Signature:
  - RSA, DSS, ECDSA and others.

PGP Services



PGP Message


Content
Operation
Session key component
Signature
Message
Key ID of recipient's public key (KU_b)
Session key (K_S)
Timestamp
Key ID of sender's public key (KU_a)
Leading two octets of message digest
Message Digest
Filename
Timestamp
Data
E_{KUb}
E_{KRa}
ZIP
E_{Ks}
R64

PGP Key Rings

- PGP supports multiple public/private keys pairs per sender/recipient.
- Keys stored locally in a *PGP Key Ring* – essentially a database of keys.
- Private keys stored in encrypted form; decryption key determined by user-entered pass-phrase.

Key Management for PGP

- Public keys for encrypting session keys / verifying signatures.
- Private keys for decrypting session keys / creating signatures.
- Where do these keys come from and on what basis can they be trusted?

PGP Key Management

- PGP adopts a trust model called the *web of trust.*
- No centralised authority
- Individuals sign one another's public keys, these "certificates" are stored along with keys in key rings.
- PGP computes a *trust level* for each public key in key ring.
- Users interpret trust level for themselves.

PGP Trust Levels

- Trust levels for public keys dependent on:
  - Number of signatures on the key;
  - Trust level assigned to each of those signatures.
- Trust levels recomputed from time to time.

THANK YOU