SNS COLLEGE OF ENGINEERING

Kurumbapalayam(Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NAAC-UGC with 'A' Grade

Approved by AICTE, Recognized by UGC & Affiliated to Anna University, Chennai

DEPARTMENT OF INFORMATION TECHNOLOGY

Course Code and Name : 19IT602– CRYPTOGRAPHY AND CYBER SECURITY

III YEAR / VI SEMESTER

Unit 5: CYBER SECURITY SAFEGUARDS AND SECURITY SERVICES

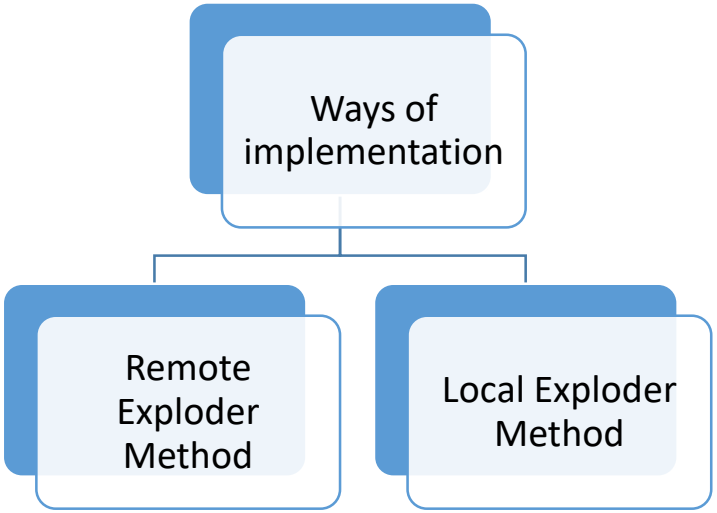
Topic : Electronic Mail security

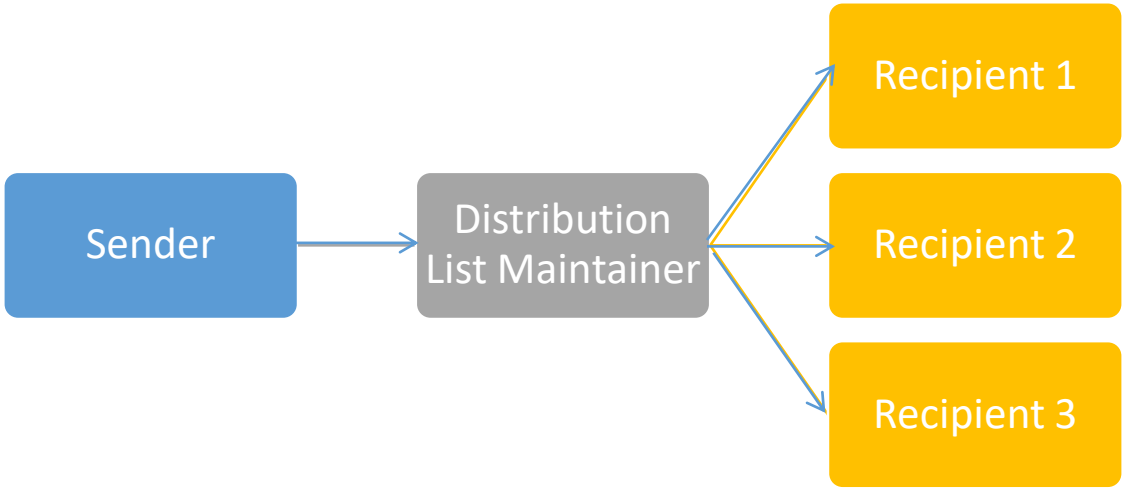
Email Security

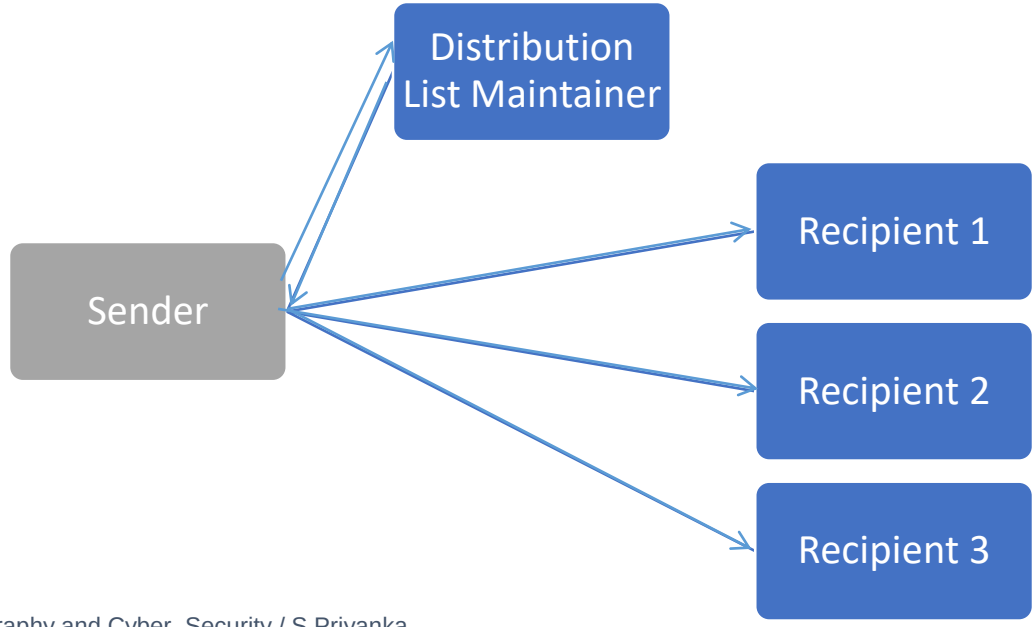
- Email is one of the most widely used
- Allows user to send messages
- Example
  - From : abc @gmail.com
  - To : cdf@yahoo.com
  - Sub: Hi How are you?

Distribution List

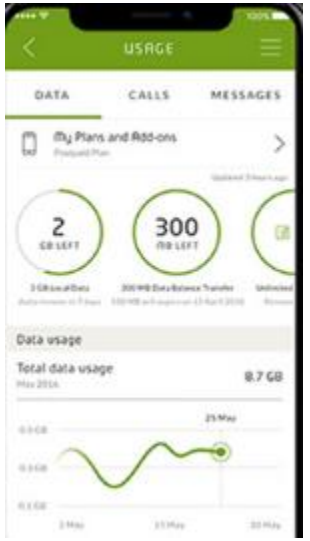
- Set of recipients







Local Exploder Method: Advantages



- Local Exploder
  - Easier to prevent mail forwarding loops.
    - Caused by distribution lists contained in distribution lists.
  - Easier to prevent multiple copies of the same message.
    - By weeding out duplicates in the list.
  - Bandwidth consumption is known to user.
    - Important when we start billing per email message.

Remote Exploder Method: Advantages

- Remote Exploder
  - Allows the membership to be kept secret from sender.
  - Can be cheaper if recipients are geographically clustered around the list maintaining site.
  - More efficient if list size is bigger than message size.
  - Faster when distribution lists are contained in distribution lists.

Possible attacks of Emails

- Phishing attack - attempt to find info like username, password either directly/indirectly
- Malware Distribution
- Spam attack- junk mail attack
- Denial of Secure attack-attacker send bulk mail either make overflow/crash

Email Security Services


CERTIFIED MAIL
eCERTIFY
Proof of Acceptance
(Electronic)
U.S. Postal Service
CERTIFIED MAIL RECEIPT
OFFICIAL USE
488 × 290


Received

Key Establishments

- Establishing Public Keys:
  - Out-of-band transmission
    - PGP public key hash on business card.
  - PKI
  - Piggy-backing of certificates on email messages
- Establishing Secret Keys
  - Out-of-band transmission
  - Ticket via KDC.
    - Alice would obtain a ticket for Bob and attach it to her message to him.

Privacy

- Threats
  - Eavesdropping.
  - Relay nodes might store messages.
    - In fact, many relay nodes log messages completely.
  - Fundamentally, at sender and receiver's machine.
    - Email there is not in transit and not protected by the Electronic Communications Privacy Act.

Privacy

- End-to-End Privacy
  - Sender and recipient use encryption.
  - Complicated by multiple recipients.
  - Keys should be only used sparingly to avoid cipher attacks.
    - Alice chooses a secret key S.
    - Alice encrypts S with the key she shares with each recipient.

To: Bob, Carol, Dexter

From: Alice

Key-info: Bob 98932472138, Carol 129834298732, Dexter 100231098432

Message: qewroiu3219087v90(87sdh32198y*&97slknseiahfusdfiu39587(*

Privacy

- With Distribution List Exploders
  - Remote exploding:
    - Alice chooses a secret key S and encodes her message.
    - Alice attaches S encrypted to all recipients.
    - Distribution list exploder decodes S and attaches it encrypted to all recipients.
      - Remote exploder knows the contents.
  - Local exploding:
    - Alice needs to exchange keys with all people on the list.

Thank You