Secure Email: Part 1

Gaurav S. Kasbekar
Dept. of Electrical Engineering
IIT Bombay

References

- J. Kurose, K. Ross, "*Computer Networking: A Top Down Approach*", Sixth Edition, Pearson Education, 2013
- A. Tanenbaum, D. Wetherall, "*Computer Networks*", Fifth Edition, Pearson Education, 2012.
- L. Peterson, B. Davie, "*Computer Networks: A Systems Approach*", Fifth Edition, Morgan Kaufmann, 2012.
- W. Stallings, "*Cryptography and Network Security: Principles and Practice*", Pearson Education, 7th edition, 2016

Motivation

- Recall:
  - ❑ some desirable properties of secure communication are confidentiality, message integrity and end-point authentication
  - ❑ we discussed several mechanisms that can be used to achieve secure communication, *e.g.*, symmetric and public key cryptography, cryptographic hash functions, digital signatures, public key infrastructure, nonces
- Next, we study several systems that use the above mechanisms to provide security in the Internet:
  1) Pretty Good Privacy (PGP) and Secure/ Multipurpose Internet Mail Extension (S/MIME) for securing email
  2) Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for securing TCP connections
  3) IPSec and Virtual Private Networks (VPNs) for network-layer security
  4) 802.11i and 802.11w for securing Wireless LANs (Wi-Fi) and systems for securing wireless cellular networks
- Note that the above systems provide security at the application layer, transport layer, network layer and link layer, respectively

Reason for Providing Security at Multiple Layers

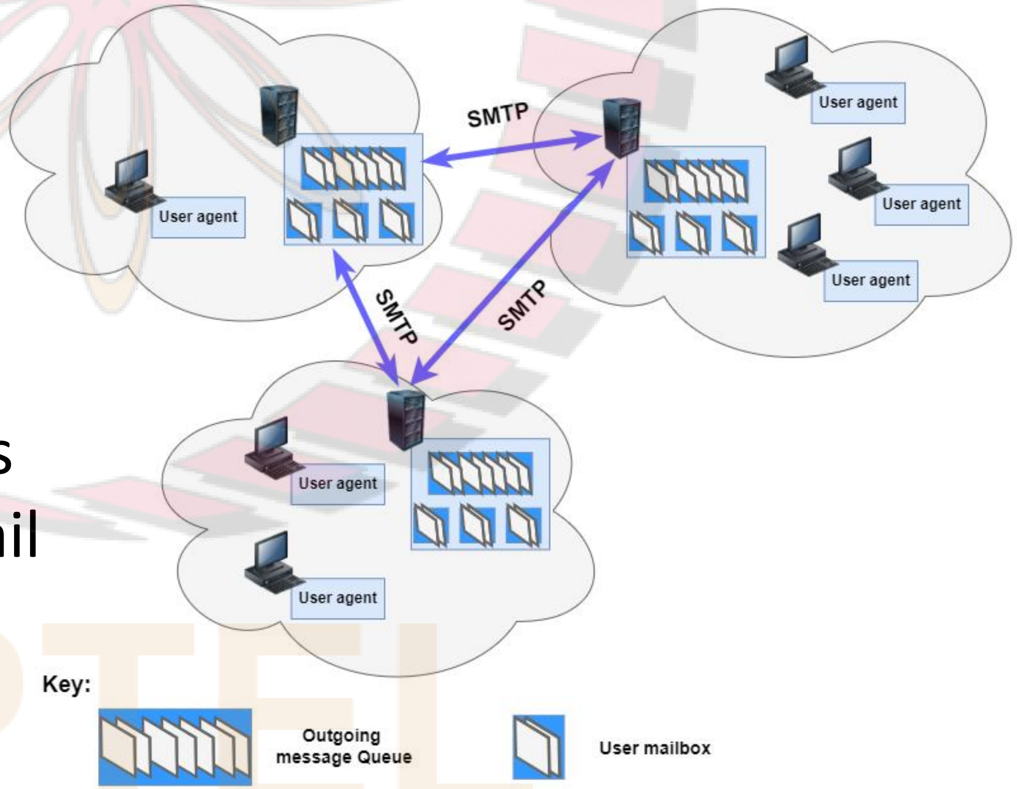
- Different kinds of attacks can be made by malicious users; security at different layers required to defend against them, *e.g.*:
  1) If a laptop user connecting wirelessly to a Wi-Fi router wants to defend against sniffing on wireless channel by intruders, sufficient to secure the wireless link (link layer security)
  2) Suppose a user wants to connect to a bank's server for an online payment; wants to check that the website is indeed bank's website and wants confidentiality from ISP employees accessing data, needs to secure transport layer
  3) Suppose a company has offices at multiple locations and wants to establish a Virtual Private Network to securely connect together all the machines in all the offices; does not want intruders on public Internet to find out amount of traffic flowing between any pair of machines; needs to secure network layer

Overview of Email in the Internet

Overview of Email in the Internet

Three major components:

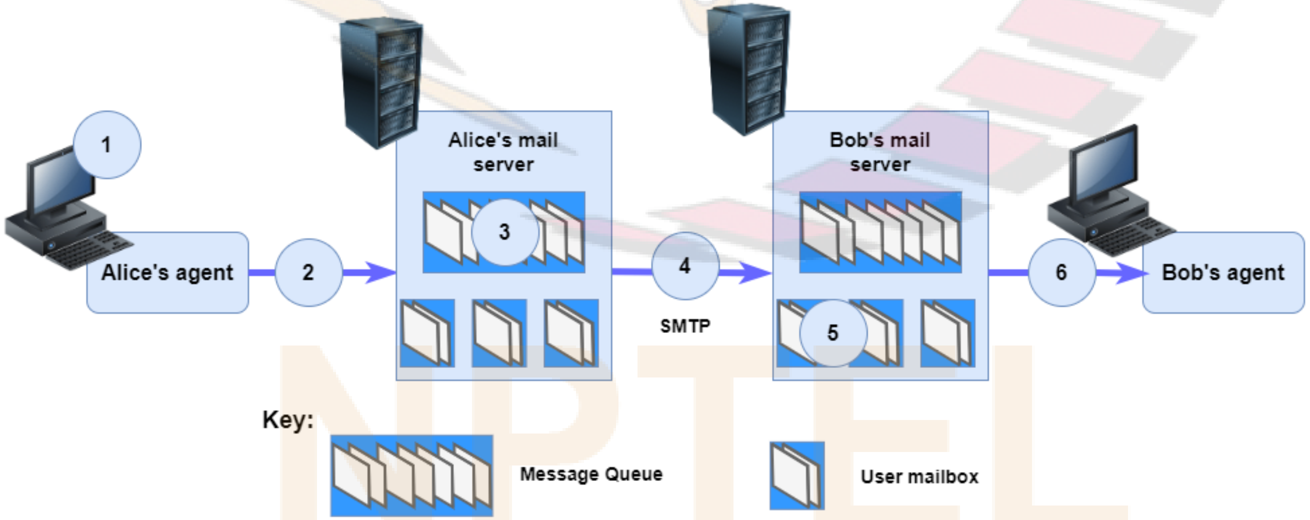
- *User agents*: allow users to read, reply to, forward, compose emails, etc. (*e.g.*, Microsoft Outlook, Pine, Gmail and SquirrelMail web interfaces)
- *Mail Servers*: where user mailboxes and outgoing message queues are stored
- *Simple Mail Transfer Protocol (SMTP)*: application-layer protocol that uses TCP to transfer email reliably from sender's mail server to receiver's mail server



Example

- Suppose Alice wants to send an email to Bob

1) Alice invokes her user agent, composes and sends an email to bob@someschool.edu
2) Alice's user agent sends the message to her mail server, where it is placed in outgoing message queue
3) Client side of SMTP, running on Alice's mail server, sees the message in the queue and opens a TCP connection to an SMTP server running on Bob's mail server
4) After some initial SMTP handshaking, the SMTP client sends Alice's message into the TCP connection
5) At Bob's mail server, the server side of SMTP receives the message and places it in Bob's mailbox
6) Later, Bob invokes his user agent and sees the email from Alice



Overview of Email in the Internet (contd.)

- SMTP has two sides: a client side and a server side
- Both client and server sides run on every mail server
- When an email is sent, client side of SMTP on sender’s mail server opens a TCP connection to server side of SMTP on receiver’s mail server and transfers email
- If a sender’s server is not able to deliver an email to a receiver’s server (*e.g.*, due to power failure at latter), then:
  - ❑sender’s server holds the message in message queue
  - ❑attempts to transfer the message later (*e.g.*, reattempts may be done every 30 minutes or so)

Pretty Good Privacy (PGP) for Securing Email

PGP

- Email security package that provides:
  - confidentiality
  - message integrity
  - compression
  - key management
- Available free of charge on Internet for various platforms including Linux, Windows and Mac OS
- **<u>Components of PGP</u>**:
  - Email data encryption using a block cipher called IDEA (International Data Encryption Algorithm); symmetric key based, uses 128 bit keys, similar to DES and AES
  - Digital signature (encrypted MD5 hash) used for message integrity
  - RSA used for securely sharing the 128 bit IDEA key and generating a digital signature for message integrity
  - Lempel-Ziv algorithm used for compression
  - Checking whether a public key indeed belongs to a specific user may be done using Certification Authorities or a “Web of Trust” (details later)

PGP (contd.)

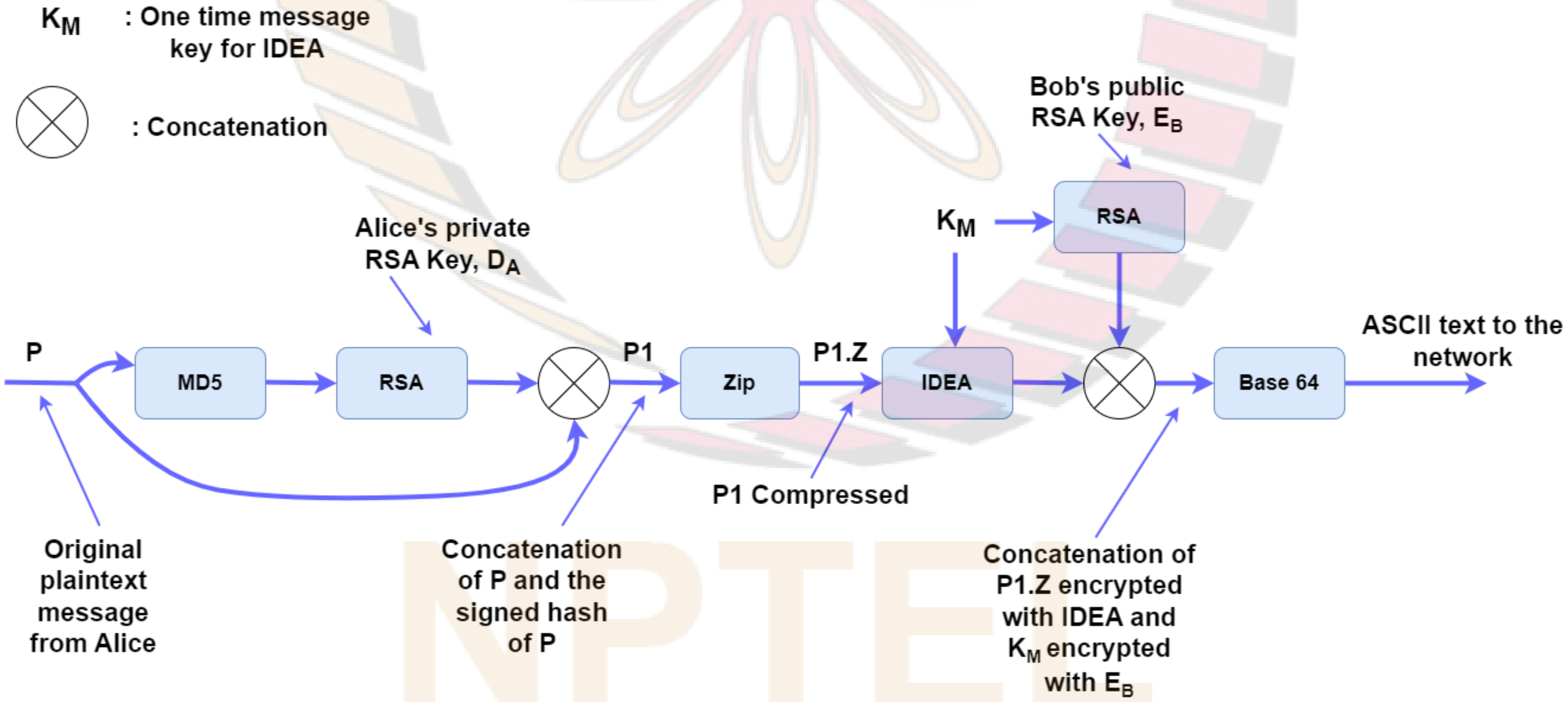
- PGP is like a preprocessor that takes plaintext as input and produces signed ciphertext as output
- The output can then be emailed using a user agent
- Example PGP message:

```
-----BEGIN PGP MESSAGE-----
Version: PGP for Personal Privacy 5.0
u2R4d+/jKmn8Bc5+hgDsqAewsDfrGdszX68liKm5F6
Gc4sDfcXyt
RfdS10juHgbcfDssWe7/K=lKhnMikLo0+1/BvcX4t=
=Ujk9PbcD4
Thdf2awQfgHbnmKlok8iy6gThlp
-----END PGP MESSAGE-----
```

- Browser plugins are available, which provide interfaces for PGP encryption and decryption for user agents (*e.g.*, Gmail)

PGP Operation

- Suppose Alice wants to send an email to Bob
- Let D_A and D_B denote Alice and Bob's private keys, and E_A and E_B denote their public keys
- Let P denote plaintext message



K_M : One time message key for IDEA
: Concatenation
P
MD5
RSA
Alice's private RSA Key, D_A
P1
Zip
P1.Z
IDEA
K_M
RSA
Bob's public RSA Key, E_B
Base 64
ASCII text to the network
Original plaintext message from Alice
Concatenation of P and the signed hash of P
P1 Compressed
Concatenation of P1.Z encrypted with IDEA and K_M encrypted with E_B