E-Mail Security

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-09/

Overview

- Email Overview: SMTP, POP, IMAP, Radix-64, MIME

- Security Services: Privacy, authentication, Integrity, Non-Repudiation, Anonymity

- Secure Email Standards: S/MIME, PGP, DKIM, …

- Spam

Internet Email Overview

❑ Simple Mail Transfer Protocol (SMTP):
Protocol to deposit email in another user's mailbox
Was originally designed for 7-bit ASCII text messages

❑ Post Office Protocol (PoP):
Protocol to retrieve email from your mailbox
Authenticates the user

❑ Internet Mail Access Protocol (IMAP)

❑ Multipurpose Internet Mail Encoding (MIME):
To encode non-text messages

| SMTP Client | SMTP | SMTP Server | | PoP Server | PoP | PoP Client |

SMTPd

PoPd
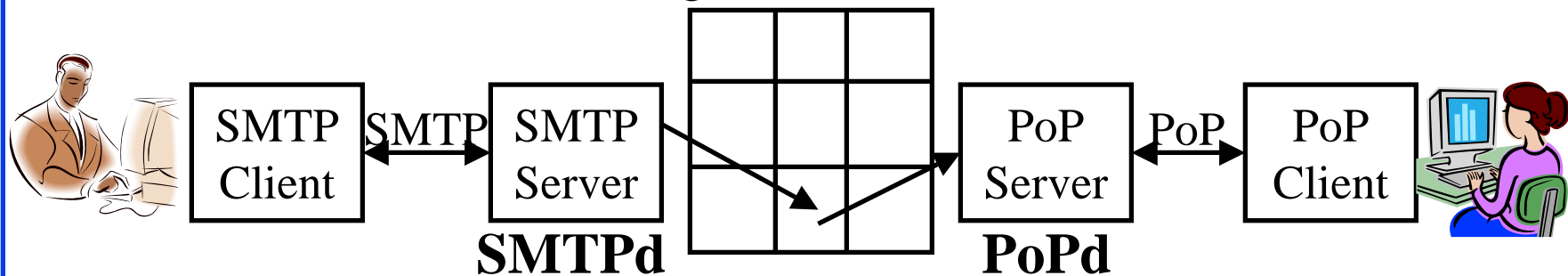
FROM:jain@wustl.edu

TO:jain@acm.org

Mail boxes
At acm.org

SMTP

❑ Defined in RFC 2821 and RFC 2822

❑ Clients connect to port 25 of SMTP server

❑ It is a push protocol and does not allow to pull

❑ Extended SMTP (ESMTP) is defined in RFC 2821

❑ ESMTP uses EHLO in stead of HELO

❑ ESMTP allows finding the maximum message size

❑ SMTP-AUTH is an authentication extension to SMTP (RFC 4954)

❑ Allows only authorized users to send email

Radix-64 Encoding
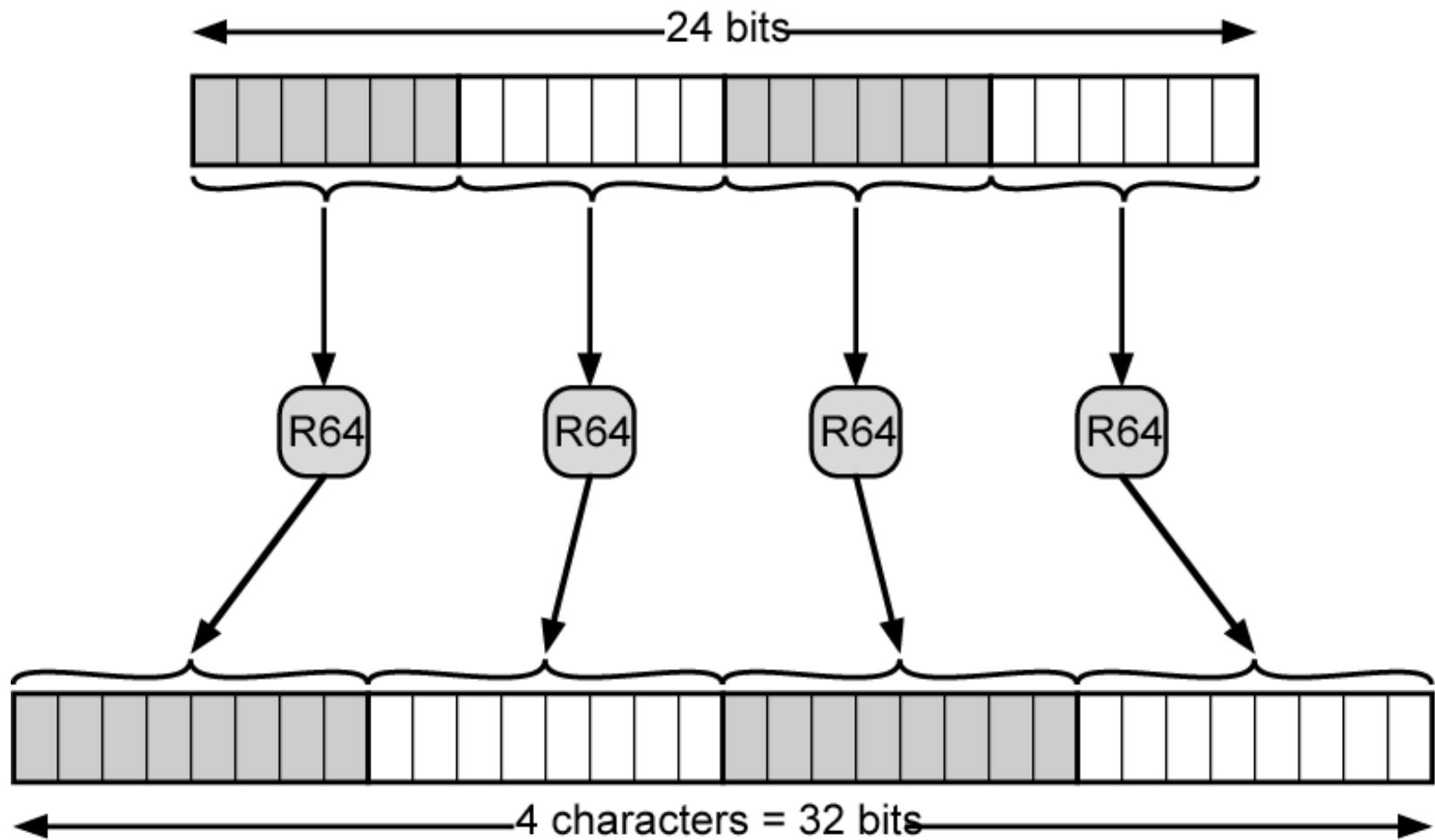
MIME Example

--unique-boundary-1
Content-Type: multipart/parallel;
boundary=unique-boundary-2

--unique-boundary-2
Content-Type: audio/basic
Content-Transfer-Encoding: base64

... base64-encoded 8000 Hz single-channel
u-law-format audio data goes here....

--unique-boundary-2
Content-Type: image/gif
Content-Transfer-Encoding: Base64
... base64-encoded image data goes here....

Security Services for E-Mail

❑ Privacy: of content

❑ Authentication: of Sender

❑ Integrity: of Content

❑ Non-repudiation: Sender cannot deny

❑ Proof of Submission: Proof of sending
  (Certified mail) – MTA can sign a message digest

❑ Proof of Delivery: to recipient
  (return receipt + Content non-repudiation)

❑ Message flow confidentiality

❑ Anonymity

Security Services for E-Mail (Cont)

❏ Containment: Keeping messages in a security zone

❏ Audit: event log

❏ Accounting: Accounting log

❏ Self Destruct: Receiving mail program will destroy the message

❏ Message Sequence Integrity: in-order delivery

Establishing Keys

❑ 1-to-1

❑ Public Keys:

 ➢ Need public key to send an encrypted message

 ➢ Can sign a message and send a certificate

❑ Secret Keys:

 ➢ Via KDC

Privacy

❑ Employee vs. Employer

❑ End-to-End Privacy

❑ Use public key to encrypt a secret key

❑ Same encrypted message can be sent to multiple recipients

❑ Distribution lists require trusting the exploder

Source Authentication

❑ Sign a hash of the message with private key (Good for distribution lists also)

❑ Secret Key:

  ➢ MAC=CBC residue with a random key

  ➢ Message digest of the random key

  ➢ Message digest is encrypted with the secret shared key (Same digest for multiple recipients)

  ➢ Can share a secret key with mail exploder

Message Integrity

❑ Generally goes with source authentication
    Integrity with source anonymity is meaningless

❑ You can use a shared secret

❑ Anyone can change the message encrypted or
    protected with public key

Non-Repudiation

❑ Public Key:

  ➢ Non-Repudiation: sender signs the message with private key

  ➢ Plausible Deniability: Sender computes a MAC using a random key S and sends $[[S]_{\text{Bob Public}}]_{\text{Alice Private}}$

❑ Secret Key:

  ➢ Non-Repudiation: Notary N. N and receipient share a secret

  ➢ N computes a seal = digest of the message and alice's name using a secret key

  ➢ N shares a secret key with recepient and sends A MAC of the message, seal, and Alice.

  ➢ A judge could ask N to verify if the seal is valid.

Proof of Delivery

❑ Delivering MTA or recipient can sign a message digest

❑ Impossible to prove that recipient got the message.

  ➢ If recipient signs it before getting the last part of the message, it may not get complete message but has signed.

  ➢ If recipient signs after getting the last part of the message, it may not sign but has the message.

Verifying Posting Date

❑ Preventing Backdating: Notary signs and dates the message

❑ Preventing Postdating: Notary signs and dates the message along with a fact not known before the date, e.g., newspaper headline, lottery number, ...

Digital Postmarks

- Post office can date stamp your document
(Service available in USA and other countries also)
- Client software signs a document and sends it to DPM service
- DPM authenticates the signature, generates a timestamp and signs the resulting package (hash of message, signature, time)
- The DPM receipt is sent to the client software and also stored in a non-repudiation database with the message and signature
- The client software wraps the original document and DPM receipt
- Anyone can verify the signature and time
- Original document can be requested from DPM service database
- www.usps.com/electronicpostmark/

Anonymity

❑ penet.fi allowed two-way communication. Assigned code name to sender.

❑ If someone replies they are also assigned a code name

  ➢ Assigned code name to the source exploder of the replies.

❑ Message Flow Confidentiality

  ➢ Can send random messages through third party

  ➢ Can use several intermediaries

Anonymous Remailers

❑ Pseudonymous Remailers: Give a pseudonym to the sender and send.

❑ Keep a log of pseudonym and actual address => Can be disclosed

❑ Cypherpunk Remailers: Removes the senders address (no return address) => No log

❑ Mixmaster Remailers: Anonymous remailer that sends messages in fixed size packets and reorders them to prevent tracing

❑ Mixminion Remailers: Strongest anonymity. Handle replies, forward anonymity, replay prevention, key rotation, exit policies, integrated directory servers, dummy traffic

Secure Email Standards

❑ Privacy Enhanced Mail (PEM) - Not deployed

❑ S/MIME - Uses PEM principles

❑ PGP

❑ STARTTLS (SMTP over TLS – RFC 2487)

❑ SMTP-AUTH (SMTP with password authentication)

❑ DKIM

S/MIME

- Secure MIME
- Originally developed by RSA Data Security Inc.
- Later control passed on to IETF
- Can use any certificate
- Bob first sends a signed message with a certificate
- Alice can then send an encrypted message to Bob
- PEM and S/MIME use X.500 names
- S/MIME requires Email as "Alternate Name" in the X.509 certificate
- Also, a new component E was added to the X.500 name

S/MIME Example

-----------boundarymarker

Content-Type: application/pkcs7-signature;
   name="smime.p7s"

Content-Transfer-Encoding: base64

Content-Disposition: attachment; filename="smime.p7s"

Content-Description: S/MIME Cryptographic Signature

ABDECDIPAQaAIHGNPAISJPDSFPSDNADNPA

-----------boundarymarker

Pretty Good Privacy (PGP)

❑ Used RSA and IDEA (RSA patent in US until 2000)

❑ V2.6.2 became legal for use within US and can be downloaded from MIT

❑ A patent-free version using public algorithm has also been developed

❑ Code published as an OCRable book

❑ Open PGP and GNU Privacy Guard

❑ Uses certificates issued by almost anyone

❑ Certificates can be registered on public sites, e.g., MIT

❑ hushmail.com is an example of pgp mail service

DomainKeys Identified Mail (DKIM)

❏ RFC 4871

❏ Sending MTA inserts a signature on behalf of the sender

❏ Verifying (Receiving) MTA verifies the signature based on public key of the sender

Spam Statistics

❑ 30 Billion spams per day (June 2005) to 90 billion spams per day (feb 2007)

❑ 80 to 85% of mail is spam

❑ Most spam originates from USA (19.6%) but 73.58% of spamvertisers are in China.

❑ Addresses are harvested from web pages, usenet groups, corporate directories

❑ Spam is sent using botnets, open relays, and open proxies

❑ Many DNS blackhole list sites were closed down due to DDoS attacks

CAN-SPAM Act of 2003

❑ Spamming is a misdemeanor
❑ You can send unsolicited commercial email iff

1. Unsubscribe compliance
   ➢ Unsubscribe mechanism
   ➢ Opt-out honored within 10 days
   ➢ Opt-out lists used only for compliance

2. Content compliance
   ➢ Accurate from, subject, advertisers address
   ➢ Identify Adult content

3. Sending behavior Compliance
   ➢ Not sent through an open relay
   ➢ Not sent to harvested address
   ➢ Cannot contain false header

Anti-SPAM:End-User Techniques

❑ Address munging: jain at wustl dot edu

❑ Avoid responding to spam

❑ Use contact forms

❑ Disable HTML in e-mail: Web bugs (1x1 transparent gifs) can identified who read the mail

❑ Disposable e-mail addresses

❑ Reporting spam: spam@uce.gov

❑ Responding to spam: Overload the advertiser

Anti-SPAM:Administrator Techniques

❑ Authentication and Reputation

❑ Challenge/Response Systems

❑ Checksum-based filtering: Matching checksum => Spam, hash busters

❑ Country-based filtering

❑ DNS Black Lists

❑ Enforcing RFC standards

❑ HELO/EHLO checking: HELO 127.0.0.1 or HELO localhost

❑ Greylisting: Error code 4xx => Retry later

❑ Fake MX Records: Multiple MX records, spammers do not retry

❑ Greeting delay: Spammers do not wait

Administrator Techniques (Cont)

❑ Hybrid filtering: Pattern matching and scoring

❑ Rule-based filtering: more general filtering and scoring

❑ Statistical content filtering: Learning from user submitted spam/ham

❑ Reverse DNS checks: Email address domain=IP address domain?

❑ Sender-supported whitelists and tags: Certified not be spammer

❑ SMTP callback verification: Check return address

Anti-SPAM: Sender ISP Techniques

❑ Background checks on new users and customers

❑ Confirmed opt-in for mailing list: Removes false submission

❑ Egress spam filtering: Check customer's email addresses

❑ Limit e-mail backscatter: bouncing messages

❑ Port 25 blocking

❑ Port 25 interception: Rate limit and egress spam filter

❑ Rate limiting

❑ Monitor Spam reports

❑ Strong Acceptable Use Policy

Anti-SPAM:Law Enforcement

❑ Honeypots

❑ Spamtraps

Summary
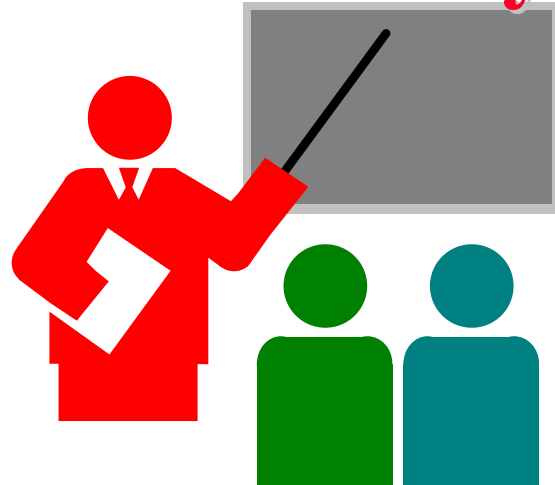
- UA, MTA, SMTP, PoP, IMAP, Radix-64, MIME
- Encryption is done using secret keys, which are sent using public key encryption
- S/MIME and PGP both use certificates
- Spam identification/reduction requires recipient, adminstrators, ISPs, and government actions

Homework 16

❑ Read chapter 20 complete, and relevant sections of 21, 22 of the textbook

❑ Try answering Exercise 20.4 and 20.7