Email Security (1)
Objectives

- Understand how e-mail systems operate over networks.
- Classify the threats to the security of e-mail.
- Study how S/MIME and PGP can be used to add security to e-mail systems.
- Examine what other security measures are needed to ensure security for e-mail systems.
- Bring together all the elements of network security to examine the security of a key application.
Contents

- Why study e-mail security?
- E-mail – what it is and how it works.
- E-mail security threats.
- Secure e-mail standards and products
  - PGP and S/MIME.
- E-mail security beyond PGP and S/MIME.
Why Study E-mail Security?

- After web browsing, e-mail is the most widely used network-reliant application.
- Mail servers, after web servers, are the most often attacked Internet hosts.
- Basic e-mail offers little security, counter to public perception.
- Good technical solutions are available, but not widely used.
  - If we understand why this is so, we might understand something about why security is ‘hard’.
- E-mail security makes a good case study for our course: a single well-defined application whose security we can evaluate.
What It Is and How It Works

- What is an e-mail?
  - RFC 822 and MIME

- How are e-mails transported, accessed and stored?
  - MUAs and MTAs
  - SMTP, POP3 and IMAP
RFC 822

- An e-mail is a message made up of a string of ASCII characters in a format specified by RFC 822 (dating from 1982).
- Two parts, separated by blank line:
  - The **header**: sender, recipient, date, subject, delivery path,…
  - The **body**: containing the actual message content.
- Use of ASCII causes problems for non-ASCII message bodies, e.g. attachments – more later.
An Example RFC 822 Message

From: Kenny.Paterson@rhul.ac.uk
To: Joe.Bloggs@rhul.ac.uk
Cc: kennypaterson@hotmail.com
Subject: RFC 822 example
Date: Fri, 15 Nov 2002 13:58:49

This is just a test message to illustrate RFC 822. It’s not very long and it’s not very exciting. But you get the point.
MIME

MIME = Multipurpose Internet Mail Extensions

- Extends the capabilities of RFC 822 to allow e-mail to carry non-textual content, non-ASCII character sets, long messages.
- Uses extra header fields in RFC 822 e-mails to specify form and content of extensions.
- Supports a variety of content types, but e-mail still ASCII-coded for compatibility.
- Specified in RFCs 2045-2049.
MIME headers

MIME specifies 5 new e-mail header fields:
- MIME-Version  (must be 1.0)
- Content-Type
- Content-Transfer-Encoding
- Content-ID  - optional
- Content-Disposition  - optional
**MIME Content-Type**

- Seven major content types with 15 sub-types.
- **Most important is** Multipart/mixed, indicating that the body contains multiple parts.
- Each part can be a separate MIME message – hence nesting of MIME messages to any level.
- Parts separated by a boundary string defined in **Content-Type** field.
Content-Transfer Encoding

- RFC 822 e-mails can contain only ASCII characters.
- MIME messages intended to transport arbitrary data.
- The `Content-Transfer-Encoding` field indicates how data was encoded from raw data to ASCII.
- `base64` is a common encoding:
  - 24 data bits (3 bytes) at a time encoded to 4 ASCII characters.
An Example MIME Message

From: j.bloggs@rhul.ac.uk
To: Kenny.Paterson@rhul.ac.uk
Subject: That document
Date: Wed, 13 Nov 2002 19:55:47 -0000
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="---next part"

---next part
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: 7bit

Kenny, here’s that document I said I’d send. Regards, Joe

---next part
Content-Type: application/x-zip-compressed; name="report.zip"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="report.zip"

rfvbnj756tbGHUSISyuhsia9982372SHHS3717277vsgGJ77JS77HFyt6GS8

---next part--
How Are E-mails Transported?

- **MUA** = Mail User Agent, *aka* Mail Client
- **MTA** = Mail Transport Agent, *aka* Mail Server
Composition and Delivery – I

- MUA = Mail client is a program running on Sender’s machine, e.g. Microsoft Outlook
- Sender supplies To: and Subject: fields and message body.
- MUA translates into RFC 822 message and connects across LAN to MTA = Mail server.
- MUA instructs MTA using a protocol called SMTP (or a proprietary alternative) and sends RFC 822 message.
Composition and Delivery – 2

- Sender’s MTA uses DNS (Domain Name Service) to find IP address of recipient’s MTA (could be local) based on To: field.
- Sender’s MTA opens connection to Recipient’s MTA and uses SMTP (Simple Mail Transfer Protocol) to instruct remote MTA and transfer RFC 822 message
  - often across public Internet.
- Intermediate MTAs may be involved.
- Recipient’s MTA may deliver to Recipient’s MUA or may store message locally for later retrieval across LAN.
Simple Mail Transfer Protocol

- Basic SMTP is defined in RFC 821, widely used for MUA-MTA and MTA-MTA conversations.
- SMTP uses TCP on port 25 for connections, so SMTP traffic carried over LAN and Internet and is (largely) unprotected.
- ‘Skilled’ user can talk SMTP directly over a telnet connection to remote MTA, supplying `From:` field of choice.
- So forging e-mail is nearly trivial (though mail headers usually give away source IP address).
Where's The E-mail?

- UNIX systems often transfer e-mail from MTA to files in local client file system.
  - Use elm, pine, xmail to read e-mail on client machine.
  - UNIX username and password controls access to client mailbox.
  - Thus security of mail system partly relies on user account security.
Where’s The E-mail? (Cont’d)

• Can also store e-mail on mail server rather than on client machine.

• Two common protocols for mail client-mail server interaction:
  ◦ POP=Post Office Protocol (RFC 1939, v3)
  ◦ Other proprietary protocols also exist.

• Username and password required before mail can be accessed
  ◦ often sent over network in clear.

• Secure extensions to POP and IMAP also exist: challenge/response based on user password.
Web-based Access

- Useful for users with web browser but no mail client, e.g. user on the road.
- Username/password combination to control access.
- Now entire client-server interaction over HTTP instead of POP/IMAP.
  - What happens to passwords in cybercafe? Keyboard sniffers?
  - Does History on browser reveal mail messages read and sent?
- Possibly protected using SSL.
E-mail Security Threats

We distinguish two kinds of threats to the security of e-mail:

**Threats to the security of e-mail itself**

**Threats to an organisation that are enabled by the use of e-mail.**

Other classifications are possible!
Not an exhaustive list of threats!
Threats to E-mail

- 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.
Threats to E-mail (Cont’d)

- Lack of data origin authentication.
  - *Is this e-mail really from the person named in the From: field?*
  - *Recall SMTP directly over telnet allows forgery of all e-mail fields!*
  - *E-mail could also be altered in transit.*
  - *Even if the From: field looks fine, who was logged in as Kenny.Paterson when the e-mail was composed?*
  - *Sharing of e-mail passwords common.*
Threats to E-mail (Cont’d)

- Lack of non-repudiation.
  - Can I rely and act on the content? (integrity)
  - If so, can the sender later deny having sent it? Who is liable if I have acted?

- Lack of notification of receipt.
  - Has the intended recipient received my e-mail and acted on it?
  - A message locally marked as ‘sent’ may not have been delivered.
Threats Enabled by E-mail

- Disclosure of sensitive information.
  - *It’s much easier to distribute information by e-mail than it is by paper and snail mail.*
  - *Disclosure may be deliberate (and malicious) or unintentional.*
  - *Disclosure may be internal or external (e-mail crosses LANs as well as the Internet).*
  - *Disclosure may be of inappropriate, sensitive or proprietary information.*
  - *Can lead to loss of reputation and ultimately dismissal of staff.*
Threats Enabled by E-mail (Cont’d)

- Exposure of systems to malicious code.
  - *Today, e-mail is the main vector by which computer viruses spread.*
  - *Self-replicating code embedded in e-mail, exploits features/vulnerabilities of e-mail client.*
    - *Visual basic script;*
    - *Javascript in html formatted e-mail;*
    - *exe attachments of dancing pigs.*
  - *Often (but not always) requires user interaction to propagate an e-mail virus.*
Exposure of systems to denial of service attacks.

- E-mail server attached to network, may be vulnerable to DoS attacks.
- More relevant with increasing dependence on e-mail as the communications tool.
- DoS on mail server may compromise other network services too.
Threats Enabled by E-mail (Cont’d)

• Exposure of *individuals* to denial of service attacks.
  ◦ *Mail bombing and excessive spam.*
  ◦ *Individuals* get so swamped by incoming e-mail that they stop reading it.
  ◦ *Switch to other communications channels (usually around the “you have 1000 unread messages” mark).*
Threats Enabled by E-mail (Cont’d)

- Spamming.
  - Misconfiguration of relaying capability allows mail server to be exploited for spamming, i.e. bulk distribution of unsolicited e-mail.
  - Guilty server can end up on Open Relay Blacklist.
  - Result is that all e-mail from that server gets blocked by mail servers using blacklist.

  - Spam wastes bandwidth and decreases productivity.
  - Hotmail and other free e-mail systems are particularly victimised by spammers.
  - 50% and more of all e-mail is now spam.
Threats Enabled by E-mail (Cont’d)

- Unauthorized access to systems.
  - Mail servers (OS and application) can have many security vulnerabilities; they are also attached to external networks.
  - Perfect target for hacker.
  - Lead to your mail server being used as attack platform on other systems (your own and other peoples’).
  - Consequent loss of reputation and potential damages claim.
Threats Enabled by E-mail (Cont’d)

- Any more threats?
Reading Assignment

- [Kaufman] Chapter 20