ECE 435 – Network Engineering
Lecture 6

Vince Weaver

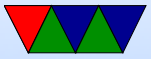
http://web.eece.maine.edu/~vweaver

vincent.weaver@maine.edu

14 September 2017

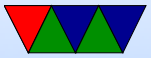
Announcements

- HW#2 was due.
- HW#3 will be posted.

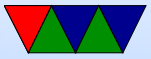


Other tools that use encryption

- How do you encrypt an e-mail, or a hard-drive, etc
- PGP – pretty good privacy
  OpenPGP RFC 4880
  Encrypt message with symmetric key, send along the key encrypted via asymmetric
  was illegal for a while (more than 40 bit encryption an exportable munition)
  people got RSA algorithm in perl tattoos
- GPG – free software replacement for PGP

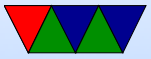


- Can also PGP sign a message. Not encrypted, but signed with your key to verify it was in fact sent by you. Takes hash of the input, then encrypts the hash with key. Also, downloads from servers (like debian)

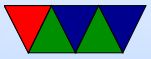


Other Encryption Concerns

- Redundancy, some way to validate plaintext is valid. Example: if encrypting a binary blob where each byte indicates something (12 34 means order 34 cows or something), random garbage might decode to valid message
- Freshness – replay attacks. What if you record old message (Bank deposits $100 to account) and replay. Will have valid encryption.
- Block chain ciphers

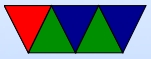


- Stream Ciphers



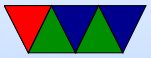
Encryption Problems

- Keys leaked (DVD/game console issues)
- poor random numbers used (Debian problem)
- differential cryptanalysis (start with similar plaintexts and see what patterns occur in output) [DES IBM/NSA story]
- Power/Timing analysis – note power usage or timing/cache/cycles when encryption going on, can leak info on key or algorithm
  Bane of perf



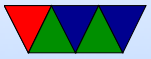
ssh security

- Fail2ban
- Nonstandard port
- Port knocking
- Call asterisk for one-time pin?
- No-password (key only)
- Two-factor authentication (LCD keyfob)



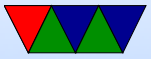
Alternatives to SSH?

- mosh



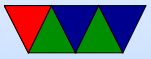
e-mail

- Been around since more or less start of networks
- ARPANET, Ray Tomlinson credited with first modern e-mail around 1971, decided to use '@' char
- UNIX mail, just a mail spool on your computer. Could use command line "mail" to send it. /var/spool/mail/username
- biff to interrupt you when mail came in (used to be exciting)
- mbox vs maildir. mbox format, tell each new e-mail via



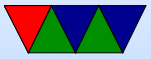
From:. So has to be escaped, you'll see this sometimes. Locking

- Want to send machine-to-machine e-mails. Various ways to do this. UUCP, etc.
- UUCP bang paths



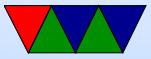
SMTP vs x.400

- As with OSI layer, the big formal ISO definition was made but the hacked-together SMTP won out.
- x.400 much better in many ways
  built-in security
  could tell you once e-mail was delivered
  can send binary files without hacks
- x.400 had horrible e-mail addresses
  C=country, A=administrator (like ISP?can be blank), P= Private Domain, etc



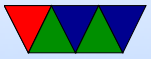
C=US;A=;P=UMaine;O=ECE;S=Weaver;G=Vince;

- x.400 actually used a lot in some situations. Microsoft exchange did for a while



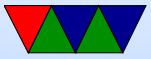
Internet e-mail

- Compose message, send to outgoing server
- deliver to mailbox, collected
- user@host.network
- can often leave off subhost, looks up mailserver for domain via DNS

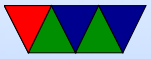


e-mail process

- Sender machine: MUA (mail user agent) sends by SMTP (simple mail transport protocol) to
- MTA (mail transfer agent) to
- Receiving MTA
- to mail delivery agent (puts into file/mailbox)
- Receive MUA on local machine via POP3/IMAP
- MUA – editor (optional) mutt/pine/thunderbird/outlook
  Often these days replaced by browser app
  can you use telnet as MUA?

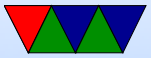


- MTA – sendmail/qmail/postfix
  speaks SMTP. sendmail was standard, has more or less incomprehensible config setup
- MDA – fetchmail? deliver mail tp mailbox. Possibly just a single file, can also be series of directories
- MCA – retrieve e-mail via IMAP or POP

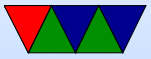


e-mail layout

- envelope
- header/body
- RFC 822/2822/5322
- originally plain 7-bit ASCII, anything more needs MIME and other extensions
- Headers
  - From:
  - Reply-to:
  - Received: (each transfer agent adds in)

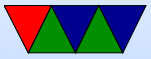


- Return-path:
- To:
- CC: (carbon copy)
- BCC: (blind carbon copy)
- Message-In:
- In-Reply-To:
- Subject:
- Date:
- X-



SMTP – simple mail transfer protocol

- connect port 25. Text. All commands 4 chars (no one remembers why)
  `S: 220 maine.edu SMTP service ready`
- `HELP`
- `HELO a.com`
  `S: 250 maine.edu says hello to a.com`
  There is an extended SMTP. You can detect by sending `EHLO` instead
- `MAIL FROM: <xyz@maine.edu>`



`S: 250 sender ok`

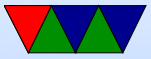
- `RCPT TO: <abx@maine.edu`

  `S: 250 recipient ok`
- `DATA`

  Put data. . on line by itself is end

  `S: 250 message accepted`
- `QUIT`

  `S: 221 maine.edu closing connection`
- Respond with 3-digit code
  - 2xx = successful
  - 3xx = flow control problem



- 4xx failed
- 5xx error in command

- In theory supposed to keep retrying to send for up to 4days