Network Security basics

CS 594 Special Topics/Kent Law School:

Computer and Network Privacy and Security: Ethical, Legal, and Technical Consideration

Recall 5-layer TCP/IP model

1. Physical layer
2. Data link layer
3. **Network/Internetwork layer** (IP)
4. **Transport layer** (TCP, ICMP, UDP)
5. **Application layer** (DNS, POP, SSL, etc.)

Why are networks vulnerable?

- Anonymity—attackers far away
- Many points of attack—both targets and origins
- Complexity of system
- Unknown perimeter—hosts come and go
- Unknown path—packet routing

TCP connection establishment

- TCP packet headers have various binary flags, including SYN (synchronize) and ACK
- Connection established via 3-way handshake:

1. Requesting host sends SYN packet
2. Accepting host send SYN/ACK packet
3. Requesting host sends ACK packet

Security implications

- That 3-way handshake occurs at Transport layer *before any* application gets access to the packet
- Hence handshake attacks *cannot* be fixed at the application layer.

Top layer: Application

- Application layer (in 7 layer model, split into 3).
- Where the protocol for the application lives
  - E.g., DNS, FTP, HTTP, IMAP and POP, SMTP, SSH, SSL
- Also where formatting values,

Application layer protocols (1)

- Application protocols need to check security, but many, especially old ones, do so poorly.
  - Telnet and ftp send passwords in the clear; rsh allows users to accept connections without password verification
    - Hence ssh for remote connections; sftp for file transfer, but ftp is still really

SSL

- **Secure Sockets Layer (SSL)** is standard application layer implementation of cryptography. (SSL 3 and TLS 1.0 are substantially the same)
- Most common use is to secure comm between web browser and web server; in this context HTTP over SSL; hence https://

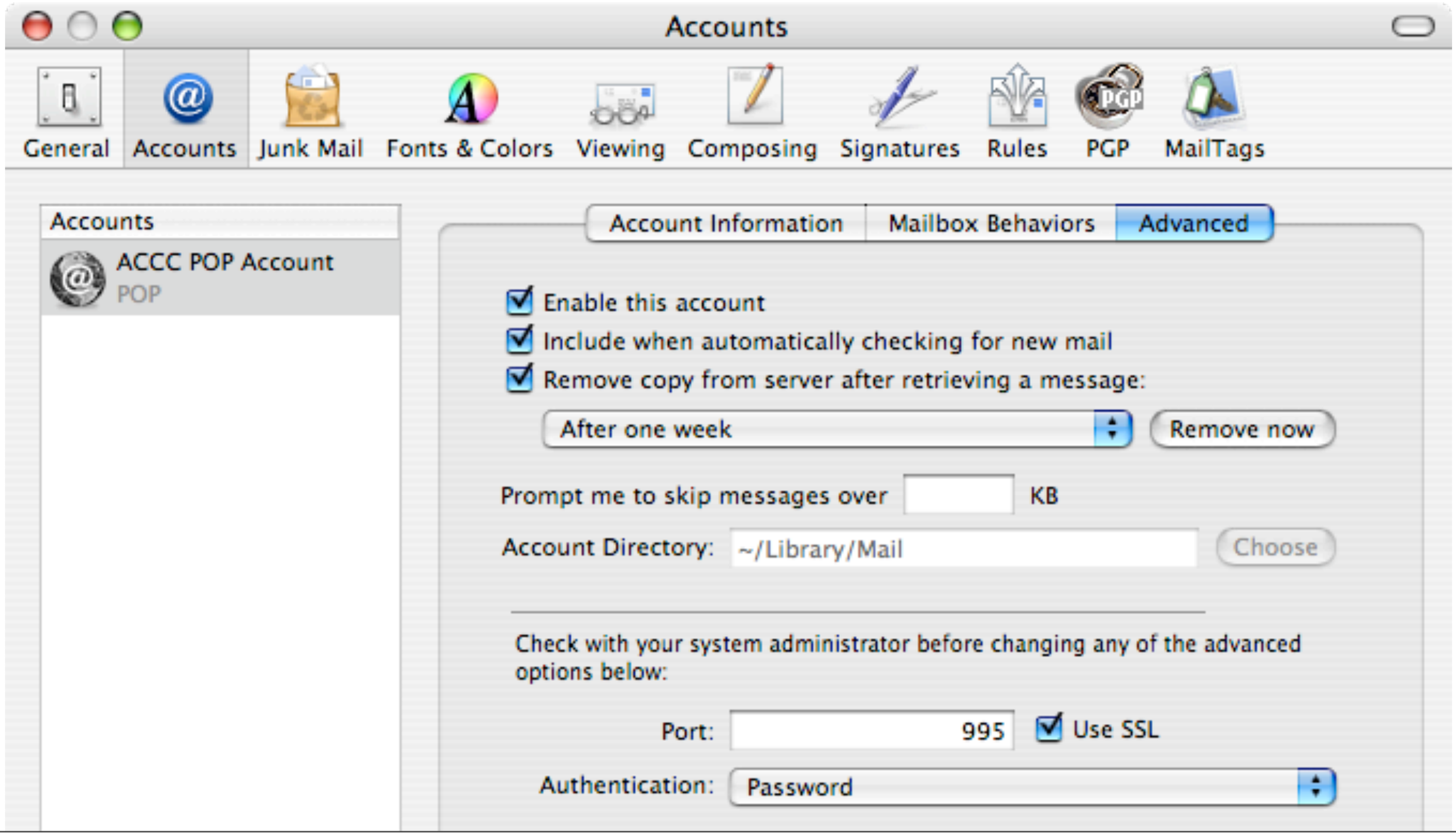
SSL continued

- SSL contains:
  - Certificates (usually only server; few if any clients have ‘em)
  - Asymmetric encryption
  - Symmetric encryption
- Session oriented

SSL and UIC

- As of May 1, 2007 UIC ACCC requires any connecting email client getting mail from mail.uic.edu use SSL connection
  - Trivial matter of a check box in most email programs.
- Issue is not the email, but your *user password*

Really easy


Accounts
General
Accounts
Junk Mail
Fonts & Colors
Viewing
Composing
Signatures
Rules
PGP
MailTags
Accounts
ACCC POP Account
POP
Account Information
Mailbox Behaviors
Advanced
Enable this account
Include when automatically checking for new mail
Remove copy from server after retrieving a message:
After one week
Remove now
Prompt me to skip messages over
KB
Account Directory:
~/Library/Mail
Choose
Check with your system administrator before changing any of the advanced options below:
Port:
995
Use SSL
Authentication:
Password

Application layer security bad; lower

- SSL/TLS, etc. must be explicitly invoked and managed by the app
  - Don't know if app did this right
  - Too high: E.g., discover TCP packet to be bogus at application layer, because it's a bad duplicate, and lower transport layer (where TCP lives) will discard good one when it finally arrives as a duplicate!

Internet future: IPSec

- Recall that Internet is running out of addresses; will be moving from IPv4 32-bit addresses to new IPv6.
- Things are/will get better at network layer: IPSec the Internet Protocol Security standard, is in limited use now; will be universal. (Optional in IPv4 but required in IPv6.)
- Provides more secure network layer: encryption of packet body; authentication of packet header.

IPSec Adds 3 protocols

- Security Associations for each connection via Internet Security Associations and Key Management Protocol (ISAKMP; RFC 2408).
  - Complex; incomplete; may change
- Authentication Headers (AH): provide packet header authentication (of host) and integrity

IPSec's 2 modes

- Transport mode: for host-to-host communication over network that may not support IPSec.
- Tunnel mode: Adds encryption of packet headers; stopping, e.g., traffic analysis; must embed packet in unencrypted packet to send

Summary

- Packet-switched network traffic can be seen, modified, or removed by attackers
- Connections can originate from anywhere in the world.
- IP source and destination addresses are world readable
- Many protocols at all levels are not security