

An Overview of Network Security (cont'd)

Copyright © 2003 Jun Li.
All rights reserved.

Upper Layers

- Messaging
 - SMTP, MIME, POP, IMAP, IM
- Internet Telephony
 - H.323, SIP
- RPC-Based Protocols
 - RPC (& rpcbind), NIS, NFS, Andrew
- File Transfer Protocols
 - FTP, TFTP, SMB
- Remote Login
 - Telnet, “r” commands, ssh
- SNMP
- Network Time Protocol
- Information Services
 - Finger, whois, LDAP, WWW, NNTP
- Proprietary Protocols
 - RealAudio, SQL*Net, etc.
- P2P
- X11
- Small Services
 - Echo, daytime, etc.

Copyright © 2003 Jun Li.
All rights reserved.

Messaging

- SMTP
- MIME
- POP
- IMAP
- IM

Copyright © 2003 Jun Li.
All rights reserved.

SMTP

- SMTP (simple mail transfer protocol) moves email on the net
- Security Issues:
 - Don't know who's the real sender
 - Can be abused for a DOS attack
 - Imagine a machine's mail spool directory is fully of junk emails
 - Privacy issues
 - EXPN, VRFY
 - Spam!
 - *Sendmail*, as the most common implementation of SMTP, is often configured badly
 - run as root on many Unix systems. :(
 - Open relay problem

Copyright © 2003 Jun Li.
All rights reserved.

MIME

- MIME (Multipurpose Internet Mail Extensions) is a protocol on encoding messages
- Security Issues
 - Structured encoded info can specify automated execution
 - Fetch a file `.ssh/identity` and `.ssh/identity.pub`
 - Can carry worms! Can carry viruses! Can carry anything!

Copyright © 2003 Jun Li.
All rights reserved.

POP

- POP (Post Office Protocol) allows a client to download messages from a mail server
 - Regularly probe the server for new emails
 - The mail will be removed from the server
- Security Issues:
 - Requires the client to have an account on the server
 - Password in plaintext in early days

Copyright © 2003 Jun Li.
All rights reserved.

IMAP

- Another protocol that provides remote mailbox access
 - Client and server can synchronize state
 - More complex than POP
- Security Issues:
 - Refer to the course material

Copyright © 2003 Jun Li.
All rights reserved.

IM

- IM (Instant Messaging) is a popular service these days
 - Proprietary protocols are used
- One security issue is the leakage of personal schedules and other info
- You probably cannot be sure who you are really chatting with
- Other security issues?

Copyright © 2003 Jun Li.
All rights reserved.

Internet Telephony

- Quite complex protocols
- H.323
 - Call traffic carried over UDP ports
 - A firewall needs to figure out what those ports are in order to allow the traffic in
- SIP
 - Either direct end to end, or through proxies
 - Call traffic carried through UDP, too

Copyright © 2003 Jun Li.
All rights reserved.

File Transfer Protocols

- TFTP (Trivial File Transfer Protocol)
 - No authentication at all!
- FTP (File Transfer Protocol)
 - A control channel (client to server)
 - A data channel
 - server to client
 - the client uses PORT command to tell the server: connect to me at port r
 - Or client to server
 - the client uses PASV command to tell server: I'll talk to you

Copyright © 2003 Jun Li.
All rights reserved.

FTP Security Issues

- Anonymous FTP area should NOT be writable
- Should not have files like /etc/passwd there
- What else?

Copyright © 2003 Jun Li.
All rights reserved.

Peer-to-Peer Networking

- All nodes are equal
 - Quite some legal issues, as you know
- Security Issues:
 - Seems every participant must be protected!
 - Seems every participant could be malicious
 - Wrong files being offered
 - Often need to allow a supplier to install and run arbitrary programs
 - What else?

Copyright © 2003 Jun Li.
All rights reserved.

The Web: Threat or menace?

- Web is hottest thing on the Internet
 - But may be one of the greatest security hazard as well

Copyright © 2003 Jun Li.
All rights reserved.