CSE/EE 461
Notes on TCP dump
Learning about http

TCPDump on attu machines

- A debugging tool used to observe network traffic
- tcpdump ordinarily requires root access
- special version tcpdump461 available on attu
- view packets on a special private network
- run server on attu
  - bind to the sniffable network address
  - function provided by support to find the sniffable address
  - sample code (serverSniff.c) demonstrates use
  - serverSniff <port> sniff
- client on attu or machine lab machine (see list)
  - use server address of attu?-461.pvt.cs.washington.edu

tcpdump461

- tcpdump461
  - only views packets on relevant ethernet card
    - ignores -i flag
  - only runs for 5 minutes
  - other limitations

tcpdump options

- man tcpdump for more info
- -x -- show messages in hex
- -xx -- show messages in hex with link level hader
- -X,-XX as above, but both hex and ascii
- -A -- print each packet in ascii minus link level header
- -D -- list the network interfaces available to tcpdump
- -i <interface> -- indicate the interface to observe
- -e -- print the link level header
- -w <file> -- write output to a file
- Optional expression to filter

tcpdump filter expressions

- No expression -- shows all packets
- port <port number> -- shows all packets going to or from the indicated port
  - dst port, src port -- only if source or destination matches port
- host <host name> -- shows all packets arriving from or going to indicated host
  - dst host, srt host -- only going to or arriving from host
- Other options to filter on type of traffic, interface used, etc.
- can combine using and, or etc.

Demo of tcpdump to observe simple client and server

Methods to find out about http

- Watch what the client does:
  - Start a simple server
  - Connect with a web browser
  - Observe how a REQUEST is made
- Watch what the server does:
  - telnet to an http server (port 80)
  - send a simple REQUEST
  - Observe the REPLY
- Observe network traffic with tcpdump
- Read the http spec.
  - http://www.w3.org/Protocols/Specs.html

Demo

- In class demo gaining info. on http

Demo

- In class demo of basic usage of gdb