Chapter 15
Networks – Part 2

ARPANet in 1969
Internet Standards and RFCs

- **Internet Architecture Board (IAB)**
  - overall architecture

- **Internet Engineering Task Force (IETF)**
  - engineering and development

- **Internet Engineering Steering Group (IESG)**
  - manages the IETF and standards process
Request For Comments (RFC)

- **RFCs** are the working notes of the Internet research and development community
Standardization Process

- Stable and well understood
- Technically competent
- Substantial operational experience
- Significant public support
- Useful in some or all parts of Internet

Key difference from ISO: operational experience
RFC Publication Process

- Internet draft
- Proposed standard
- Experimental
- Draft standard
- Internet standard
- Historic

- IETF
- IESG

- < 6 months
- > 6 months
- > 4 months

- Two independent implementations
How To Find RFCs

- http://www.rfc-editor.org/rfcsearch.html
  - Search for RFCs
- Some Popular Ones:
Modern Life In Cyberspace...

- http://www.aclu.org/pizza/images/screer

...All I Wanted Was A Pizza!
Introduction to Network Security
Security Attacks

BRINGING CIVILIZATION TO ITS KNEES...

Goths

Hack

Vandals

Hack

Hack

Huns

Hack

Hack

Geeks

Hack

Hack

Hack

Hack

Copyright © 2006 by Charlotte Observer
Security Services

- **Confidentiality** – protection from passive attacks
- **Authentication** – you are who you say you are
- **Integrity** – received as sent, no modifications, insertions, shuffling or replays
Security Services

• **Nonrepudiation** – can’t deny a message was sent or received
• **Access Control** – ability to limit and control access to host systems and apps
• **Availability** – attacks affecting loss or reduction on availability
Network Security Model
Network Security Model

Four basic tasks in designing a security service:

- **Design** algorithm
- **Generate** secret information to be used
- Develop methods to **distribute** and share info
- Specify a **protocol** to be used by the two principals
Protocols – Simple To Complex
Protocols in a Simplified Architecture
Protocol Data Units in TCP/IP

Application Byte Stream

TCP Segment

IP Datagram

Network-level Packet

Network Header

UDP Datagram

IP Header

TCP Segment

UDP Segment

TCP Header

User Data

User Data

User Data

User Data

User Data

User Data

User Data

User Data

User Data
Operation of a Protocol Architecture

DSAP = destination service access point
DHost = destination host
TCP and UDP Headers
IP Headers

(a) IPv4 Header

(b) IPv6 Header

- QoS
- 32-bit field
- max # allowable hops
- 128-bit field
TP/IP Concepts
Some TCP/IP Protocols
# Assigned Port Numbers

<table>
<thead>
<tr>
<th>Port</th>
<th>Service</th>
<th>Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>echo</td>
<td>110</td>
<td>pop3</td>
</tr>
<tr>
<td>20</td>
<td>ftp-data</td>
<td>119</td>
<td>nntp</td>
</tr>
<tr>
<td>21</td>
<td>ftp</td>
<td>123</td>
<td>ntp</td>
</tr>
<tr>
<td>23</td>
<td>telnet</td>
<td>389</td>
<td>ldap</td>
</tr>
<tr>
<td>25</td>
<td>smtp</td>
<td>443</td>
<td>https</td>
</tr>
<tr>
<td>39</td>
<td>rip</td>
<td>500</td>
<td>isakmp</td>
</tr>
<tr>
<td>53</td>
<td>DNS</td>
<td>520</td>
<td>rip2</td>
</tr>
<tr>
<td>80</td>
<td>http</td>
<td>1812</td>
<td>radiusauth</td>
</tr>
<tr>
<td>88</td>
<td>kerberos</td>
<td>2049</td>
<td>Sun NFS</td>
</tr>
</tbody>
</table>
Configuration of TCP/IP
Alternate Routing Diagram

(a) Topology

Route a: X ® Y
Route b: X ® J ® Y
Route c: X ® K ® Y
Route d: X ® I ® J ® Y

○ = end office
○ = intermediate switching node

(b) Routing table

<table>
<thead>
<tr>
<th>Time Period</th>
<th>First route</th>
<th>Second route</th>
<th>Third route</th>
<th>Fourth and final route</th>
</tr>
</thead>
<tbody>
<tr>
<td>Morning</td>
<td>a</td>
<td>b</td>
<td>c</td>
<td>d</td>
</tr>
<tr>
<td>Afternoon</td>
<td>a</td>
<td>d</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>Evening</td>
<td>a</td>
<td>d</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>Weekend</td>
<td>a</td>
<td>c</td>
<td>b</td>
<td>d</td>
</tr>
</tbody>
</table>
Ethereal

- **Ethereal** is a free network protocol analyzer for Unix and Windows
- **Packet Sniffer** - data can be captured "off the wire" from a live network connection
- **www.ethereal.com** - Everything you ever wanted to know about ethereal
- **wiki.ethereal.com** - This is the “User's Manual;” also has has a nice “References” section
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>38.984733</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>TCP</td>
<td>1126 &gt; 80 [SYN] Seq=103417 Ack=0 win=8192</td>
</tr>
<tr>
<td>53</td>
<td>39.068380</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>TCP</td>
<td>80 &gt; 1126 [SYN, ACK] Seq=354713864 Ack=104193</td>
</tr>
<tr>
<td>54</td>
<td>39.068987</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>TCP</td>
<td>1126 &gt; 80 [ACK] Seq=103418 Ack=354713865</td>
</tr>
<tr>
<td>55</td>
<td>39.085030</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>HTTP</td>
<td>POST /news_titles.asp?action=news_titles</td>
</tr>
<tr>
<td>56</td>
<td>39.180178</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>HTTP</td>
<td>HTTP/1.1 100 Continue</td>
</tr>
<tr>
<td>57</td>
<td>39.338830</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>TCP</td>
<td>1126 &gt; 80 [ACK] Seq=104193 Ack=354713954</td>
</tr>
<tr>
<td>58</td>
<td>39.758173</td>
<td>VCOSTA_LAPTOP</td>
<td>151.108.114.202</td>
<td>DNS</td>
<td>Standard query PTR 163.55.185.205.in-addr.arpa</td>
</tr>
<tr>
<td>59</td>
<td>39.758227</td>
<td>VCOSTA_LAPTOP</td>
<td>ns1.srv.hcvlny.cv.net</td>
<td>DNS</td>
<td>Standard query PTR 163.55.185.205.in-addr.arpa</td>
</tr>
<tr>
<td>60</td>
<td>39.804710</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK</td>
</tr>
<tr>
<td>61</td>
<td>39.805912</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK</td>
</tr>
<tr>
<td>62</td>
<td>39.806051</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>TCP</td>
<td>1126 &gt; 80 [ACK] Seq=104193 Ack=354716874</td>
</tr>
<tr>
<td>63</td>
<td>39.807134</td>
<td>VCOSTA_LAPTOP</td>
<td>205.185.55.163</td>
<td>HTTP</td>
<td>HTTP/1.1 200 OK</td>
</tr>
</tbody>
</table>

Frame 55 (829 on wire, 829 captured)

Arrival Time: Mar 14, 2001 01:38:22.1334
Time delta from previous packet: 0.016043 seconds
Time relative to first packet: 39.085030 seconds
Frame Number: 55
Packet Length: 829 bytes

0220 68 65 0d 0a 43 6f 6f 66 6f 66 69 65 3a 20 52 44 49 44
0230 46 68 65 73 74 61 32 39 33 31 30 2d 39 30 35 30 33 30
0240 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
0250 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
0260 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
0270 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
0280 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
0290 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
02a0 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
02b0 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
02c0 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
02d0 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
02e0 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
0300 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
0310 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
0320 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33
0330 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33 31 30 33

DNS query

Cookie is captured

Getting a quote

business.nytimes.com

ACK
Ethereal Etiquette

• Be careful when and where you use this tool
• It makes people nervous
• Use prudence with the information you collect
• **When in doubt, seek permission!**
Network Access Security Model

Opponent
—human (e.g., cracker)
—software
(e.g., virus, worm)

Access Channel
Gatekeeper function

Information System
- Computing resources (processor, memory, I/O)
- Data
- Processes
- Software
- Internal security controls
Information Security

- Physical
- Administrative
- “Lockup the file cabinet”
Private Networks

- Isolated to individual organizations
- Emergence of computer security
- Sharing a system
- Protecting data
Networking

- Networks start talking to each other
- Gateways
- Arpanet
- TCP/IP Everywhere
- Vinton Cerf, “IP On Everything!”
Maturing of the Internet

- Telephones used by 50% of world's population
- Internet attains similar level of growth by 2010 – max growth
- Connecting computers and programmable devices
- More devices than people
Early Hacking

- Cap’n Crunch cereal prize
- Giveaway **whistle** produces 2600 MHz tone
- Blow into receiver – free phone calls
- “Phreaking” encouraged by Abbie Hoffman
- Doesn’t hurt anybody
Captain Crunch

- **John Draper**
- `71: **Bluebox** built by many
- Jobs and Wozniak were early implementers
- Developed “EasyWriter” for first IBM PC
- High-tech hobo
- White-hat hacker
The Eighties

- 1983 – “War Games” movie
- Federal Computer Fraud and Abuse Act - 1986
- Robert Morris – Internet worm -1988
- Brings over 6000 computers to a halt
- $10,000 fine
- His Dad worked for the NSA!!!
It Got Worse

- 1995 – Kevin Mitnick arrested for the 2\textsuperscript{nd} time
- Stole 20,000 credit card numbers
- First hacker on FBI’s \textit{Most Wanted} poster
- Tools: password sniffers, spoofing
- \url{http://www.2600.com}
Just because you’re paranoid, doesn’t mean they’re not out to get you!

- Anonymous
Firewalls

Figure 15.8 A firewall protecting a LAN
Firewalls Make It To The Movies
Why Firewalls?

- **Internet connectivity** is no longer an option for most corporations
- The Internet allows you access to worldwide resources, but... ...the Internet also allows the *world* to try and access your resources
- This is a **grave risk** to most organizations
Why Firewalls?

- A **firewall** is inserted between the premises network and the Internet
- Establishes a **perimeter**
- Provides a **choke point** where security and audits can be imposed
- Single computer system or a set of systems can perform the **firewall function**
Good Fences Make Good Neighbors – Robert Frost, “Mending Wall”
Design Goals

• **All traffic**, from inside to outside and vice versa, must pass through the firewall

• **Only authorized traffic** (defined by the security policy) is allowed to flow

• Firewall is **immune to penetration** – uses a trusted system
Other Types Of Firewalls

- **Personal Firewalls Appliances** – personal firewall appliances are designed to protect small networks such as networks that might be found in home offices

- **Provide:** print server, shared broadband use, firewall, DHCP server and NAT

(NB: This is not an endorsement of any product)
Viruses
Viruses

- A **virus** is a submicroscopic parasitic particle that infects cells in biological organisms.
- Viruses are non-living particles that can only **replicate** when an organism reproduces the viral RNA or DNA.
- Viruses are considered **non-living** by the majority of virologists
- [www.virology.net](http://www.virology.net)
Viruses

- **Viruses**: code embedded within a program that causes a copy of itself to be inserted in other programs and performs some unwanted function
- *Infects* other programs
- *Code* is the *DNA* of the virus
Worms

"Computer Worm" Copyright John S. Pritchett
Worms

- **Worms**: program that can replicate itself and send copies to computers across the network and performs some unwanted function.
- Uses *network connections* to spread from system to system.
Useful Websites

- http://www.rfc-editor.org/rfcsearch.html
  Search RFCs
- http://www.cert.org
  Center for Internet security
- http://www.counterpane.com/alerts.html
  Some recent alerts
Assignment #3

- Research these two RFCs: **RFC1129** and **RFC968**. Given a **brief** - paragraph, not a single sentence – **description** based on the abstract, introduction, or basic content.

- Pick **google.com** and one other site. Using **whois** and **ARIN**, get as much information as possible about the IP addressing, the DNS and the site (location, owner, etc.).

- **Due next Wednesday, December 6** – or you can email it earlier.
Homework

• Read Chapter Fifteenth – and review slides

• ...Next Class We'll Cover Artificial Intelligence...
...Have A Nice Weekend

“The City” At 1200 Feet In December