Network Security: The Principles of Threats, Attacks and Intrusions (Part 1)

APRICOT 2004
Tutorial, 24 February 2004
Kuala Lumpur

Ray Hunt, Associate Professor (Networks and Security), University of Canterbury, New Zealand


gibbleguts.com
HACKERS
INFORMATION HIGHWAY

Contents

- Background to security risks and the Internet
- TCP/IP vulnerabilities
- Attack Trends
- Classification of attacks
  - Social Engineering
  - Hacking or Cracking
  - Viruses and Worms
  - Trojan Horses

  } *Blended Attacks*

  - Network Layer Attacks - spoofing, hijacking
  - (Distributed) Denial of Service Attacks

Live tests reported in “Cryptogram” (B. Schneier) www.counterpane.com

- A random computer on the Internet is scanned dozens of times a day
- The life expectancy of a default installation of Red Hat 6.2 server, or the time before someone successfully hacks it, is less than 72 hours
- A Windows home user with file sharing enabled, was hacked five times in four days
- Systems are subjected to NetBIOS scans an average of 17 times a day
- The fastest time for a server being hacked: 15 minutes after plugging it into the network

Quote from Kevin Mitnick ….

- “It's naive to assume that just installing a firewall is going to protect you from all potential security threats. That assumption creates a false sense of security which can be worse than having no security at all.”

Security and the Internet ……

- Between February 2000 and December 2001 we have seen….
- The biggest Denial of Service Attack in the history of computing (7-11 February 2000)
- The biggest Virus Attack in the history of computing (“I Love You”, 4 May 2000)
- The biggest Worm Attack in the history of computing (Nimda, 18 Sept 2001)

Security and the Internet ……

- Lion Worm Ver 0.11 released March 29, 2001
- Release of the Code-Red Worm July 19, 2001
  - Infected 359,000 computers in 14 hours
  - At peak 2000 computers were being infected per minute
- Release of Nimda Worm on 18 September 2001
  - Infected 160,000 at peak
  - within one day 450,000 unique IP addresses were attempting to spread the worm
- …. Leading to some of the most dangerous web server attacks ever known (18 September 2001)

Significant Vulnerabilities in 2002

- Gigger Worm - JavaScript virus attacks Microsoft Outlook, Microsoft Express and IRC
- Buffer overflow problems with Internet Explorer 5.01, 5.5 and 6.0 and IIS 4.5 and 5.1
- DOS problems in Microsoft's IIS 4.0, 5.0, 5.1, Cisco's ADSL routers, SNMPv1, and DNS Bind v9

Providing you are not using Microsoft Outlook, Microsoft Express, Internet Explorer, IRC, SNMP Network Management, DNS Bind or any of Microsoft's web servers since IIS 4.0 - you should be OK!!

Significant Vulnerabilities in 2003

- 25 January, 2003 - SQL Server (Slammer) Worm
  - Small MS SQL Worm (376 bytes) replicates itself using a buffer overflow technique.
  - When worm gains control it generates random IP Address and send itself by connecting to remote UDP port 1434
  - Large number of attempts leads to Denial of Service attack
  - www.ravantivirus.com/virus/showvirus.php?v=164
  - www.cert.org/advisories/CA-2003-04.html

Significant Vulnerabilities in 2003

- 16 July, 2003 - Buffer Overflow in Windows RPC and XP Shell - Severity Rating: *High*
  - RPC Buffer overflow in RPC allows attacker to gain absolute control of a Windows machine!!
  - XP Buffer overflow allows attacker to execute code with logged-in user's privlidges!!
  - Both of these are severe and a rating of "high" has not been seen for over a year
  - www.watchguard.com/archive/images/lsglossary.htm#rpc

Significant Vulnerabilities in 2003

- 17 July, 2003 - Denial of Service in *all* Cisco IOS Routers - Severity Rating: *Critical*
  - Critical DOS vulnerability which affects all Cisco IOS software running on all Cisco routers
  - By sending a specifically designed IPv4 packet to a router, all data can be blocked.
  - Although this attack is specific to IPv4 and not IPv6 most people are still running IPv4
  - This is a very significant and dangerous attack and a rating of “critical” has not been seen for over two years
  - www.watchguard.com/archive/images/lsglossary.htm#dos

Significant Vulnerabilities in 2003

- 11 August, 2003 - Blaster - Severity Rating: *Critical*
  - W32.Blaster.worm - simple worm that exploits one of the worst Windows vulnerabiities in recent history
  - Utilised critical flaw reported on July 16 to create new blended attack
  - Does not even have to use e-mail to spread
  - Exploits DCOM (Microsoft's distributed object management tool) buffer overflow with TCP port 135 (Microsoft's RPC Location Service) to gain full control of machine
  - Uses TFTP to download msblast.exe and alters regisry settings to ensure it runs every time machine is rebooted

Case Examples of Buffer Overflow in recent months

Examples from both Windows and Unix/Linux

- MS Blaster.Worm — Buffer overflow in RPC / DCOM process
- CDialog — Linux script interpreter
- XV — Unix image program
- Microsoft SQL — LPC service

Case Study - Blaster

- 8 August, 2003 Major Corporate Network Disabled with Blaster (name withheld)
  - All access to off-site web servers stopped 8 August. No apparent reason
  - Numerous tests carried out over 4 hour period by disconnecting various parts of the corpotate intranet
  - The Blaster worm was discovered but the patches had autodownloaded a few minutes too late
  - Port 135 (as used by Microsoft Web Servers was disabled on all machines). Hence no services like windows updates
  - Outage -10 hours
  - Cost to repair - $30,000 (*excluing* time spent patching servers in user departments an lost productivity)

Significant Vulnerabilities in 2003

- 23 August, 2003 - SoBig.F - Severity Rating: *Critical*
  - One of the most widespread viruses known
  - Crippled e-mail services. 57% of all e-mails infected on 21 August (21.6 of 38 million scanned by AOL that day)
  - Many large corpoates in Asia hit as well as international organisations such as Air Canada, CXS Corp. etc
  - Designed to turn computers into spam relay machines
  - Contained an encrypted file which has 20 key IP addresses to be used for large DDOS attack

Case Study - SoBig.F

- 23 August, 2003 Major Corporate Network Disabled with SoBig.F (name withheld)
  - Microsoft patches applied to all servers but it was not clear why the patch only worked in some cases and no indication of the reason it did not stick
  - Subsequently discovered that patch would only install correctly if cetain service packs were in place and backtracking on service packs often left a corrupted system file which stopped the blaster patch from working (see note)
  - Microsoft released a patch for the patch!!
  - EVERY machine in network had to be patched
  - In mean time 20-40K e-mails per day had to be filtered
  - Estimated cost to organisation $25,000

Significant Vulnerabilities in 2004

- 26 January 2004 - MyDoom email virus - Severity Rating: *High*
  - 100 million infected e-mails in 36 hours
  - Mass mailing and peer-to-peer file sharing worm that drops copies of itself into windows system directory
  - Contains its own SMTP engine to construct outgoing messages
  - Contains a Denial of Service payload
  - Can generate random e-mail subjects, message bodies and attachment file names
  - contains executable attachments (22K zip file)

Watch this space - its not over yet!!

TCP/IP and the Internet ……

- TCP/IP was designed early in the 1980s when security was hardly an issue
- TCP/IP (version 4) therefore has virtually no security facilities, yet …..
- TCP/IP is today used in virtually every:
  - local area, metropolitan, wide area, global network, and..
  - application (conventional, voice, multimedia, etc …)
- Scale of access (address, time) is unprecedented

Attack Incident Trends*

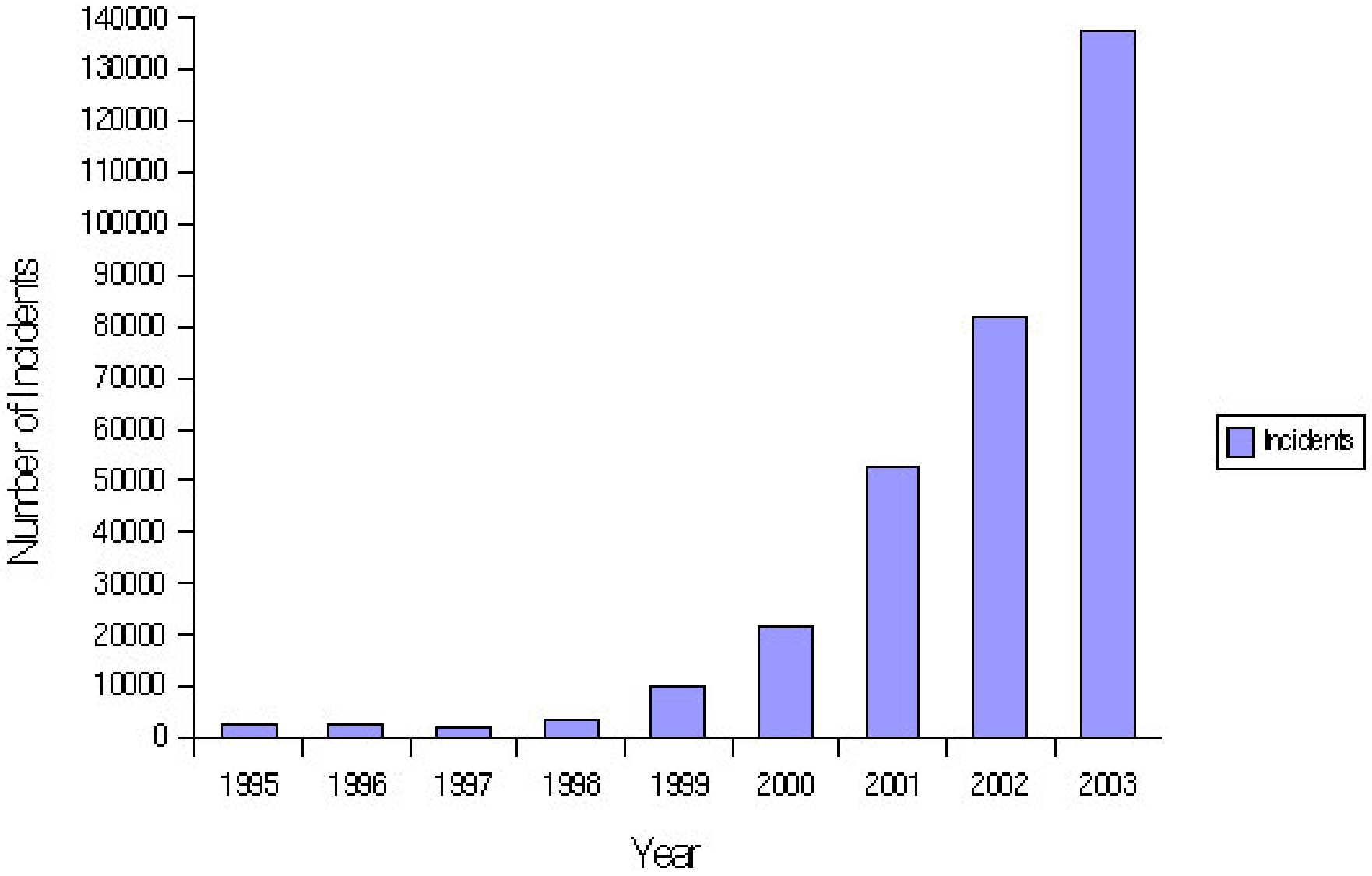
- Organisations Reporting Incidents
  - 1997 37%
  - 1999 33%
  - 2002 67%
- Where they attack
  - Internal Systems - 28%
  - Internet Access - 60%
  - Remote Dial In - 18%
  - Other - 7%

* Source: 2002 Australian Computer Crime and Security Survey

Factors Affecting Attack Trend

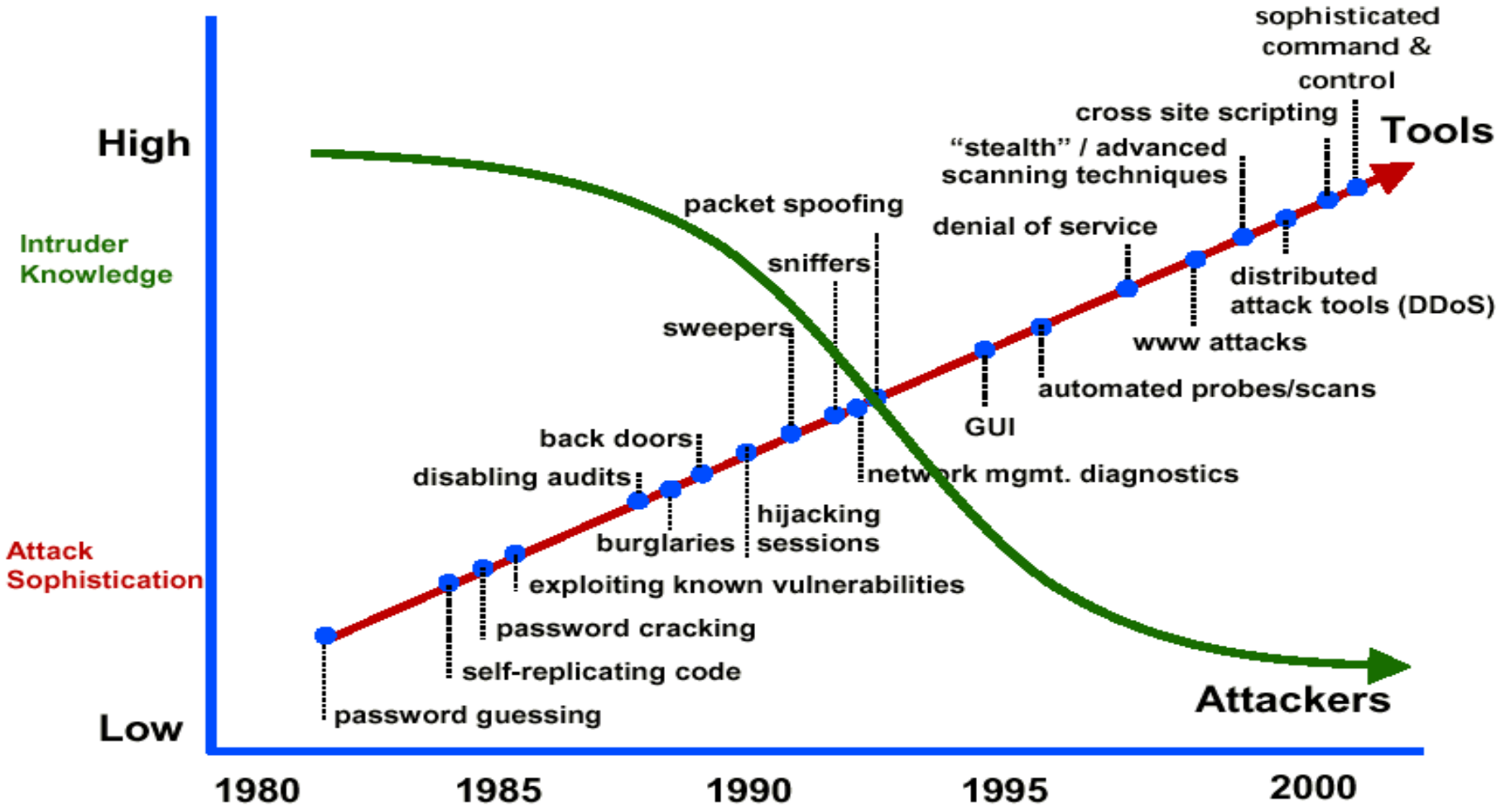
- Increased use of the Internet
- Increasing software complexity
- Abundance of attack tools
- Increased use of broadband home access
- Slow adoption of good security practices

Rise of Attack Incidents



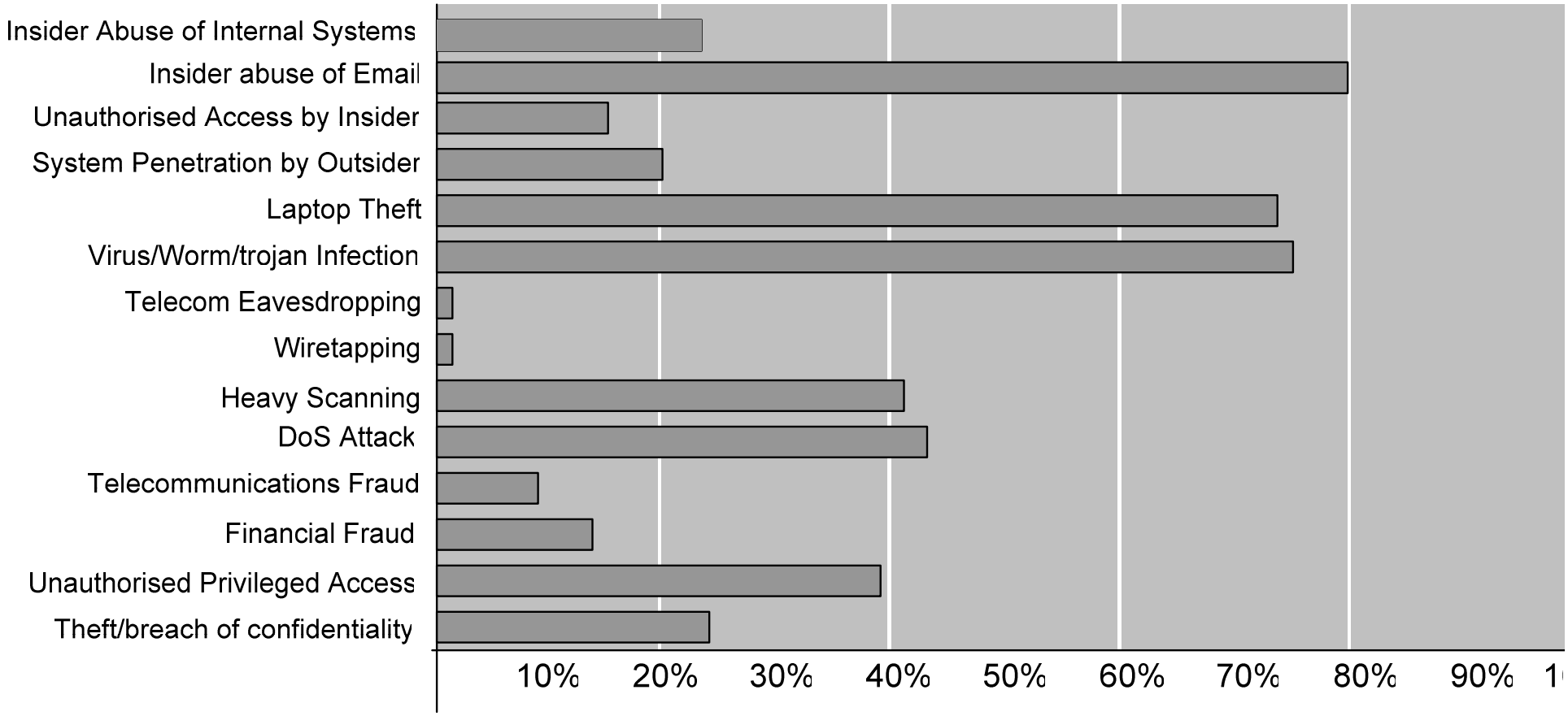
Rise in Incidents Reported to the CERT/CC - www.cert.org/stats (2004)

Rise of Attacks -
Attack Sophistication vs Intruder Tech Knowledge

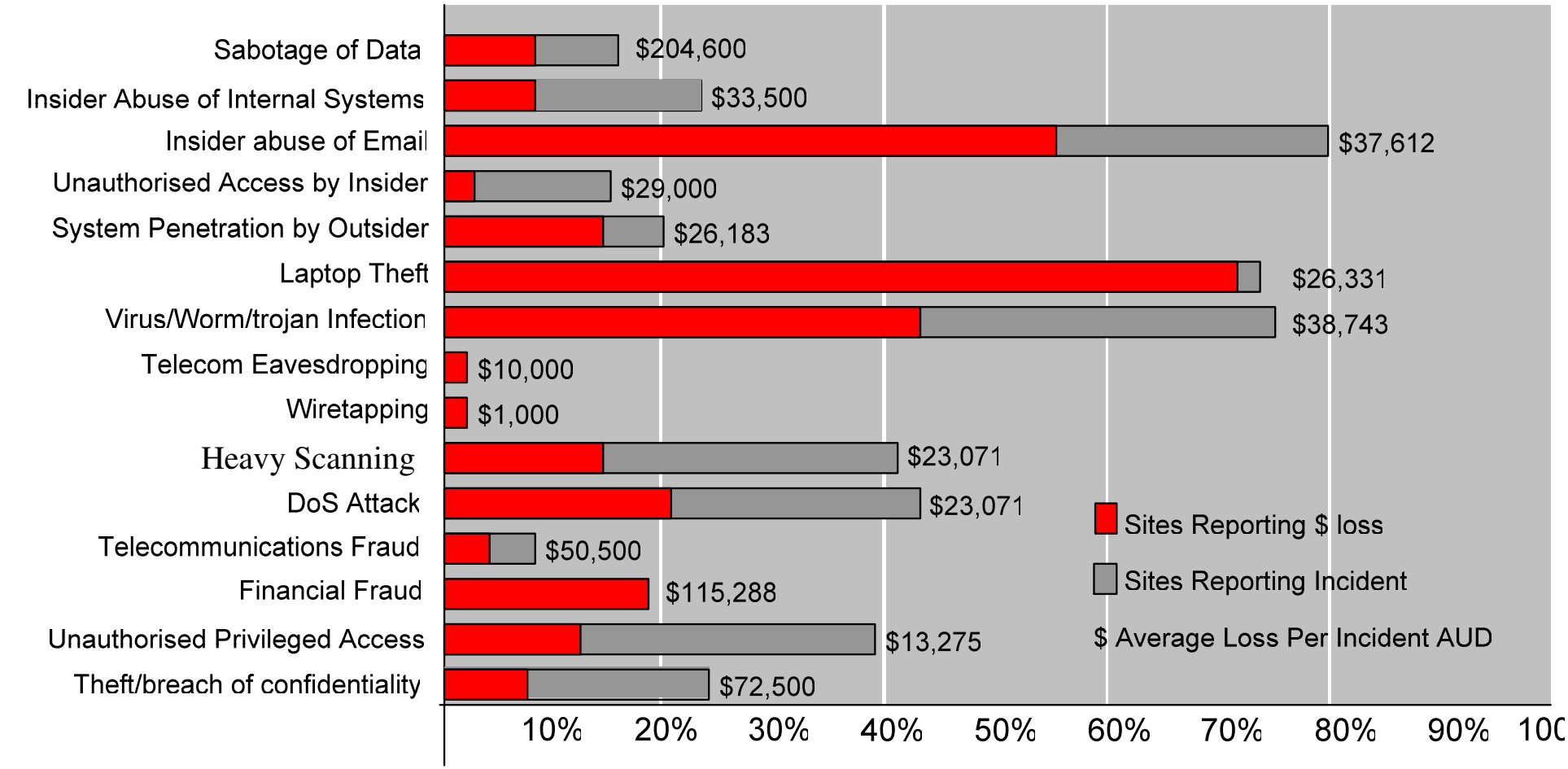


Howard Lipson. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. CERT Coordination Center. Nov. 2002

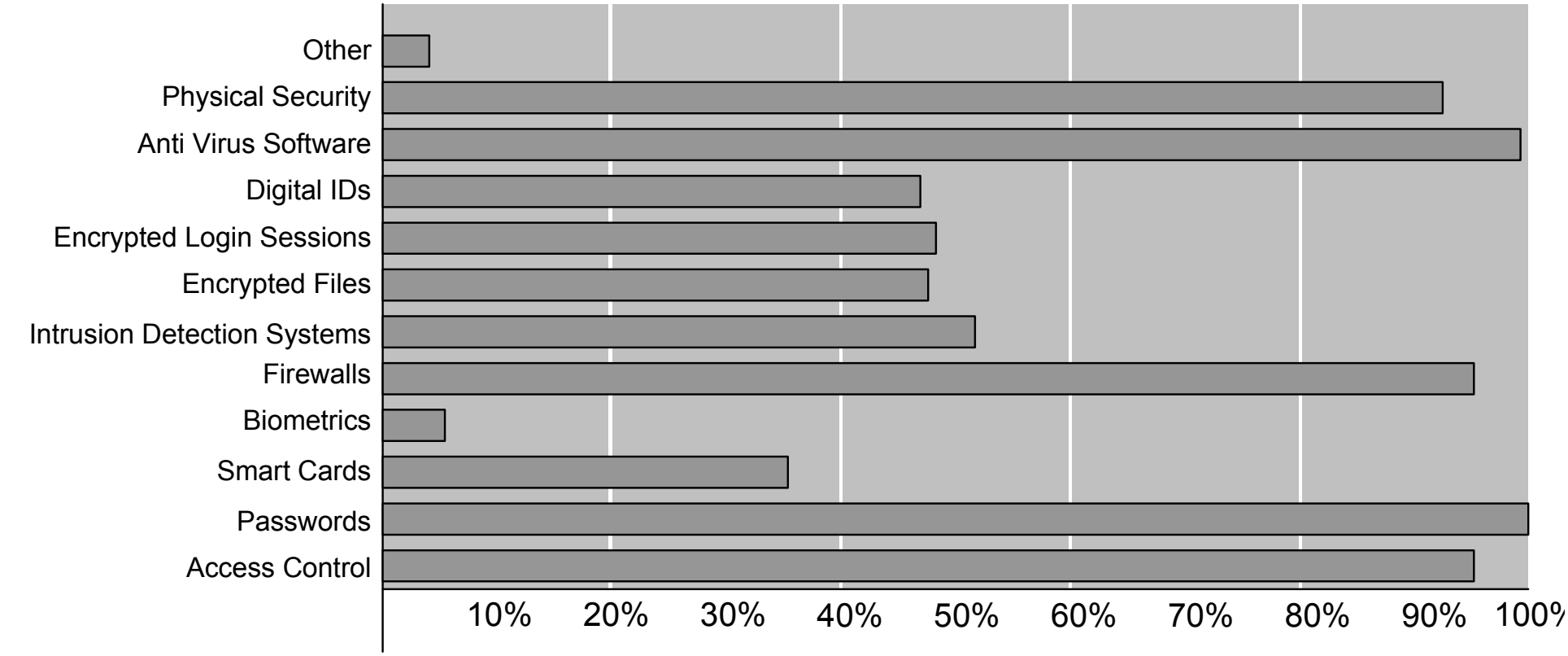
Types of Attack



Cost of Attack

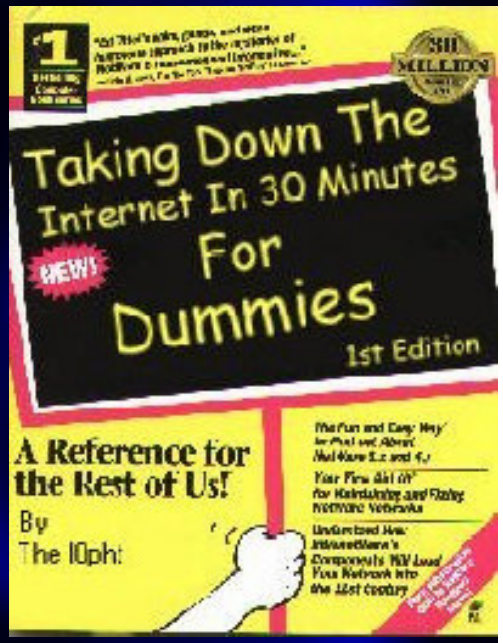


Attack Protection Systems



Classification of Attack Methods

- Social Engineering
  - Persuading somebody to ….
- Hacking or Cracking
  - Guess, corrupt or steal information
- Viruses and Worms
  - Viruses - Melissa, AnnaKournikova, SoBig
  - Worms - Lion, Ramen, Code-Red, Nimda, Blaster, MyDoom (2004)
- Trojan Horses
  - Back Orifice, PKZIP3, SubSeven etc

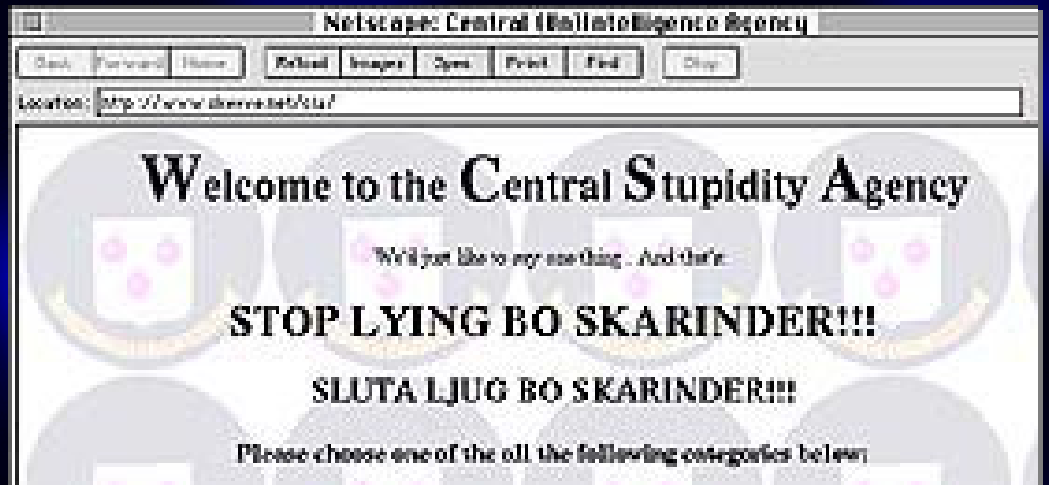


Classification of Attack Methods

- Network Layer Attacks
  - IP spoofing (masquerading)
  - Sequence number prediction
  - TCP hijacking

Classification of Attack Methods

- (Distributed) Denial of Service Attacks
  - Operating system attacks
    - Ping of Death, Tear Drop, Land, Snork, Bonk …
  - Network attacks
    - SYN flood, TCP fin/rst, Smurf, Coke ….
  - Preventing DOS attacks
  - Distributed DOS (DDOS) attacks



Threats to TCP/IP Services

- Simple Mail Transport Protocol (SMTP)
- Telnet
- Network Time Protocol (NTP)
- Finger/Whois
- Network File System (NFS)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- ActiveX
- Secure Shell (SSH)
- Domain Name Service (DNS)
- NetBIOS
- Server Message Block (SMB)

Social Engineering

- Persuade someone to disclose sensitive information (eg Nigerian Letter Scam)
- Persuade someone to run/install malicious or subverted software
- Impersonating new employee who has forgotten userid/password
- Impersonating a technical support staff member and requesting a user login to ‘check’ accounts

Hacking and Cracking

- Password guessing or written down
- Default passwords (guest, manager ….)
- Password Cracking Tools, readily available from the Internet for a wide range of password protected systems: UNIX password files, Word documents, ZIP files, Windows password files, etc
- Complete set of attack tools at: “Church of the Swimming Elephant”. www.cotse.com

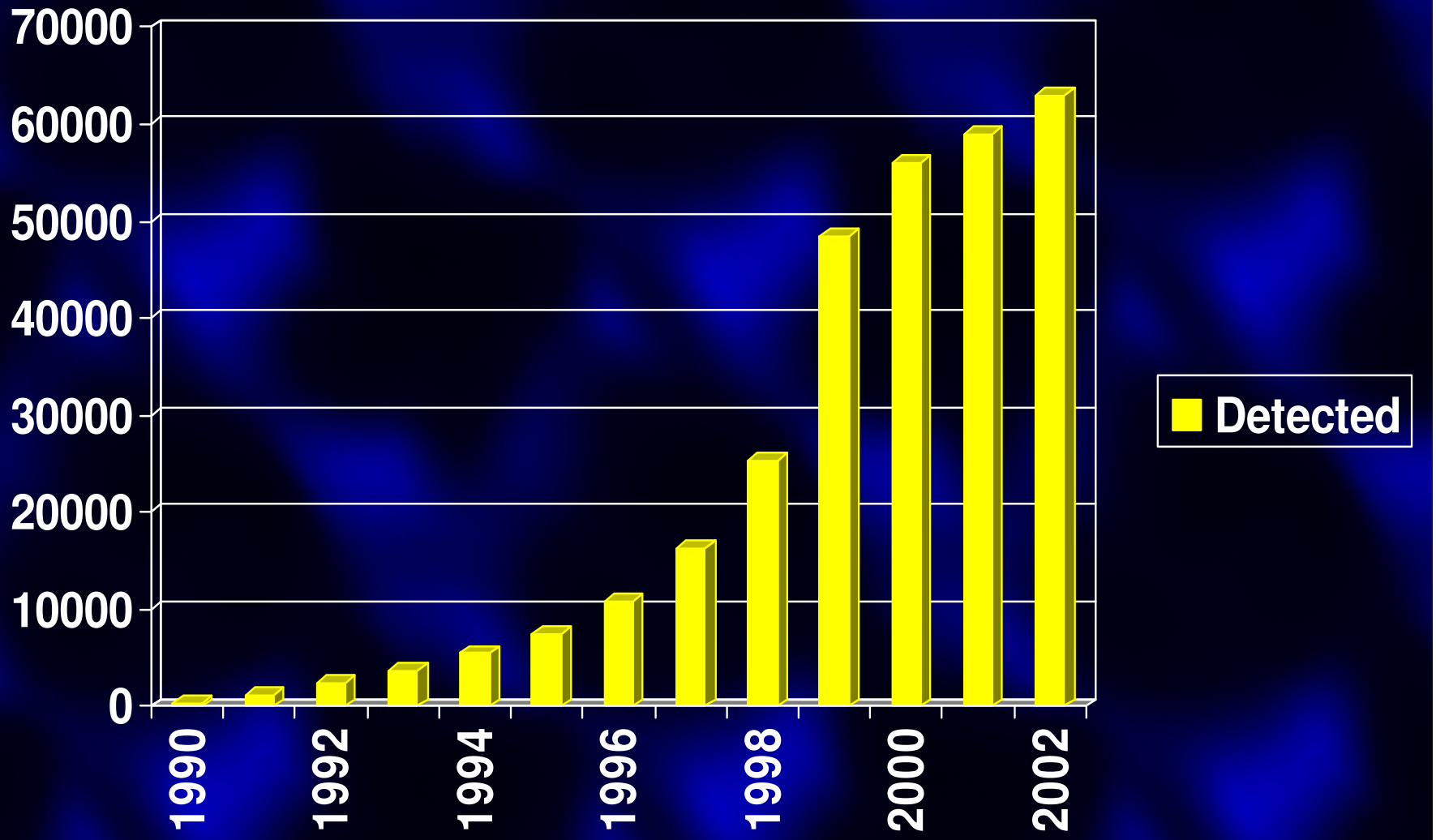
Hacking and Cracking

- Password Attacks
  - Brute Force (for few characters) and Dictionary (for real-word password) attacks
  - CRACK is available at: ftp://ftp.cert.org/pub/tools/crack
  - Can often find 10% of passwords
  - Demonstrates value of OTPs (One Time Passwords)

Hacking and Cracking

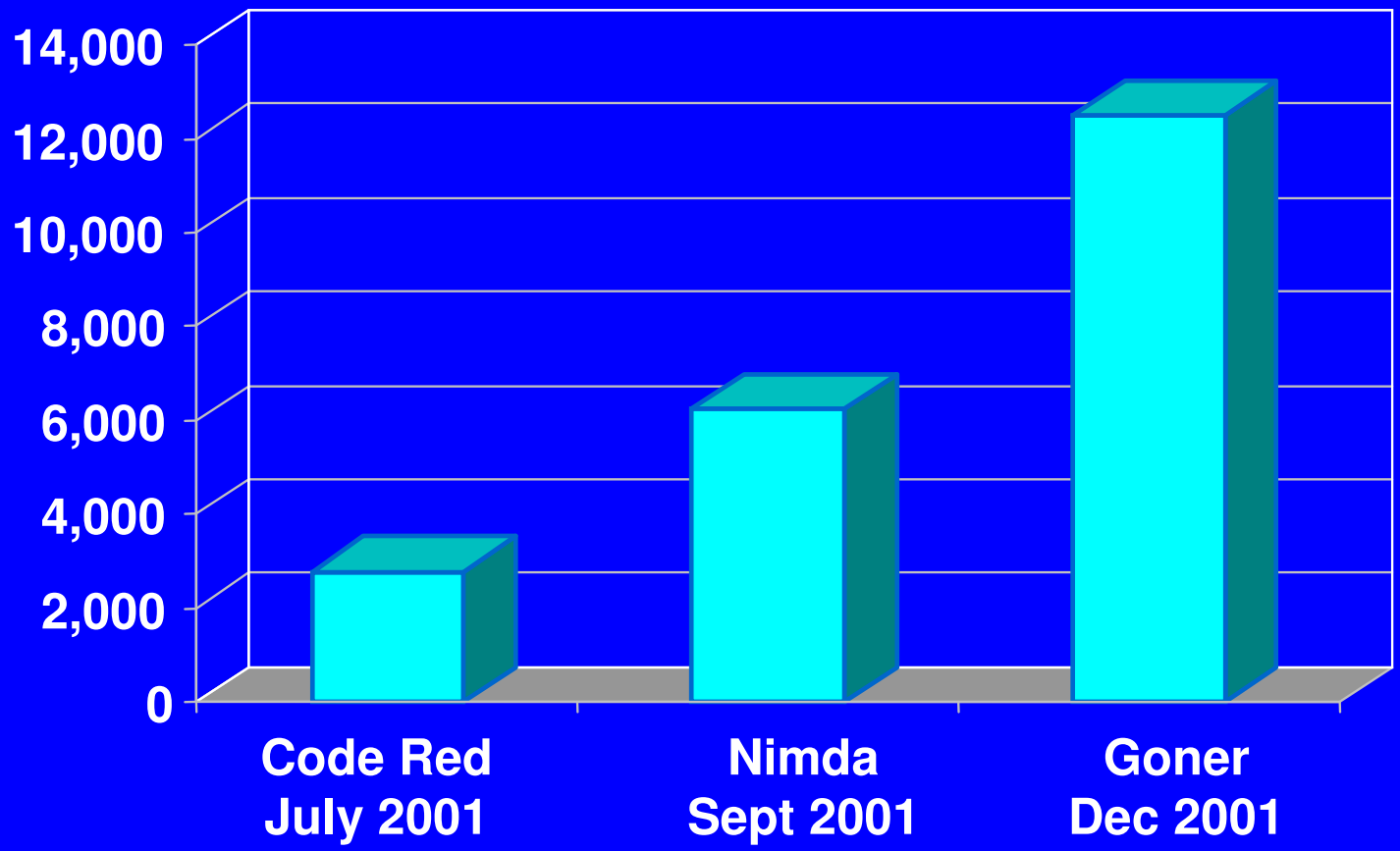
- Packet Sniffers
  - Sniffers can be legitimate tools - eg Microsoft's Protocol Analyser, Ethereal
  - Difficult to distinguish between legitimate and illegitimate use
  - Usually monitor all IP traffic
  - Demonstrates value of OTPs

Virus, Worm ... Count Increasing



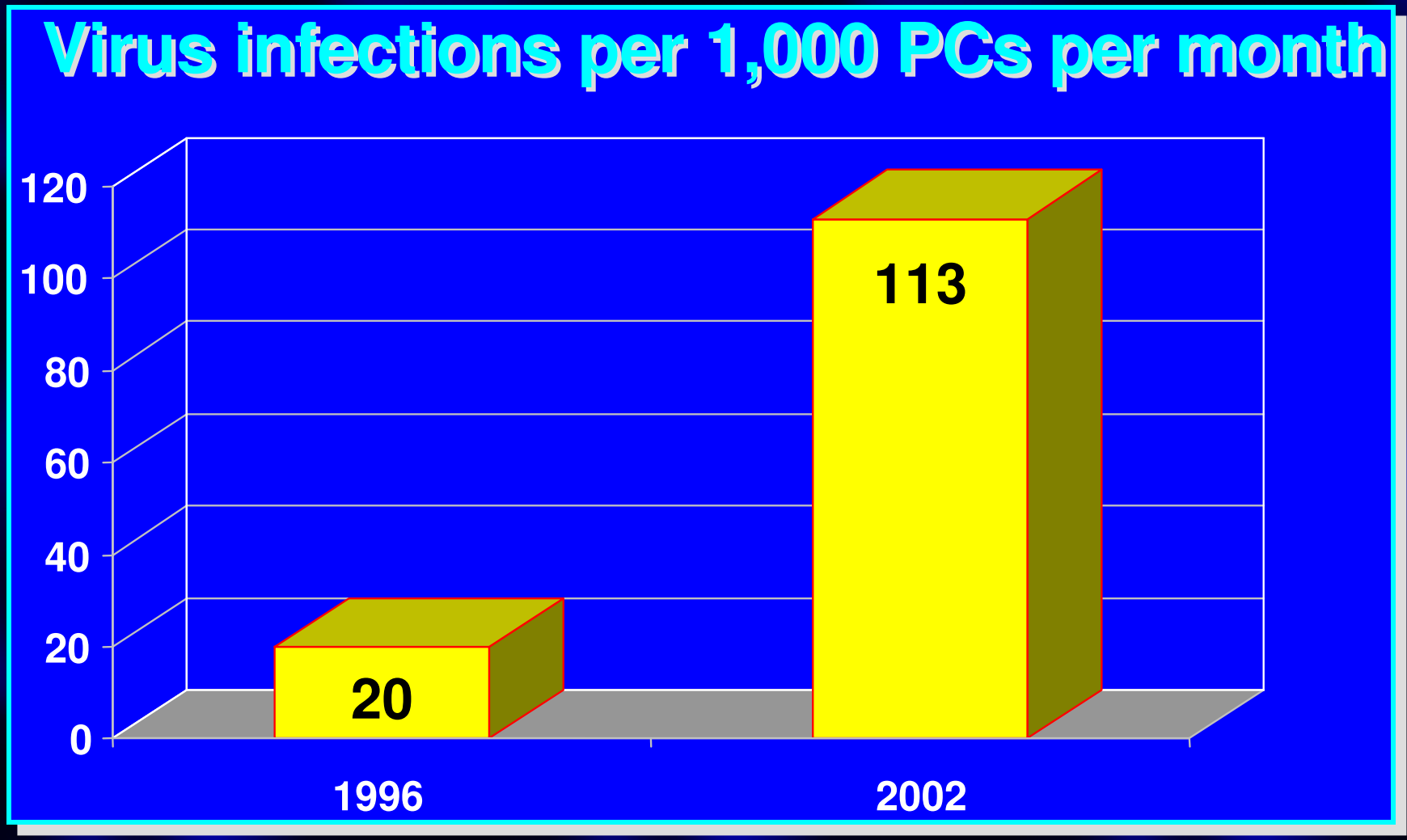
NOTE These figures include viruses, worms and other malicious code

Machines infected per hour at peak of outbreak



Source: McAfee AVERT 2001-2002

PC Infection Rate Increasing



Source: ICSA 2002

Viruses, Worms and Network Propagation Systems

- Viruses (Definition in “notes”)
  - Malicious program that spreads by infecting various files
  - When infected file is opened, virus runs its program first and then opens the (now infected) file
  - Most viruses spread by transferring infected file from one computer to another via e-mail attachments

Viruses Categories

- File infection viruses
  - attach themselves to .exe, .com, etc. (Many are DOS hangovers)
  - Polymorphic viruses change their appearance each time an infected program is run
- System or boot sector viruses
  - infects executable code, eg DOS boot sector
- Macro viruses
  - infects Microsoft Word, eg Melissa (www.melissavirus.com)
- E-mail viruses usually carried by attachments

Virus Protection

- Effective protection is anti-virus S/W which:
  - scans e-mail attachments
  - checks for virus signatures
- Examples:
  - Norton (www.norton.com)
  - McAfee (www.mcafee.com)
  - Sophos (www.sophos.com)

  Most of these have versions which provide "push" technology and update a customer's site automatically

Viruses, Worms and Network Propagation Systems

- Worms (Definition in “notes”)
  - Mass-Mailing Worms
    - do not infect files but propagate via file transfer (eg e-mail attachments) which then release a virus upon opening (eg MyDoom, 2004)
  - Network-Aware Worms
    - exploits security vulnerabilities such as unprotected shared drives, vulnerabilities in FTP etc usually by forcing a buffer overflow
    - examples - Ramen, Lion and Code-Red worms

Worm Protection

- Mass mailing worms
  - filter attachments and apply anti-virus software
- Network-aware worms
  - application of patches to fix security holes
  - Use of personal firewalls can assist
    - Zone alarm, (www.zonelabs.com)
    - Tiny firewall, (www.tinysoftware.com)
    - SyGate (wwww.sygate.com)
    - IPCop (Linux) (www.ipcop.com)
    - Smoothwall (Linux) (www.smoothwall.org)
  - Intrusion Detection System software

Lion Worm (29/3/2001)

- Infects Redhat LINUX machines
- Attacks port 53 (DNS) and installs a trojan which e-mails the /etc/passwd and /etc/shadow files to huckit@china.com
- Then deletes /etc/hosts.deny lowering the security
- Protection: See
  - www.sans.org/y2k/lion_protection.htm, March 2001

Ramen Worm (17/1/2001)

- Infects Redhat LINUX 6.2 and 7 machines
- Attacks an RPC or ftpd service
- Patches available for current versions of LINUX
- Protection: See
  - www.securityfocus.com/archive/78/157627 (bugtraq)
  - www.symantec.com/avcentre/vinfodb.html (general)
  - http://service1.symantec.com/sarc/sarc.nsf/html/Linux.Ramen.Worm.html (specific)

Code-Red Worm (19/7/2001)

- Infects all unprotected versions of Microsoft's IIS web server
- 359,000 machines attached in first 14 hours (peak infection rate was 2000/minute)
- Protection: See
  - www.securityfocus.com (bugtraq)
  - www.symantec.com/avcentre/vinfodb.html
  - www.caida.org/analysis/security/code-red

Nimda -The Mother of all Worms

('Admin' spelt backwards!)

- 18 September 2001
- Within 24 hrs -100,000's computers, 10,000's companies, 15 countries
- Generates own list of IPs then probes for IIS servers
- Utilised Code Red II worm affected machines
- Utilised 16 known vulnerabilities in Microsoft IIS
- Generates 16 HTML requests to non-patched IIS servers up to 13 times from each infected computer
- Modifies system files and registry keys
- Travels though shared drives and computers
- Creates administrator account on infected machine
- Attached to URL's infecting unsuspecting browsers

Case Study - Nimda Worm

- Attacks IIS servers that were not patched up to SPK6a (NT4) and SPK2 (Windows 2000)
- On our firewall we had 24,000 attempted connections at 2am and firewall failed (Automatic download of SophoS worm patch blocked)
- Once the worm reached the trusted network it infected IIS servers *behind* the firewall
- Attacks by issueing multiple “get” requests for files such as root.exe, cmd.exe, admin.dll
- Protection: See
  - www.securityfocus.com (bugtraq)
  - www.symantec.com/avcentre/vinfodb.html
  - www.caida.org/dynamic/analysis/security/nimda

Keeping Up-to-Date with Attacks ..

- www.cert.org/advisories (main index by year)
- www.wildlist.org (virus spread data)
- www.securityfocus.com/news (bugtraq)
- www.symantec.com/avcentre/vinfodb.html
- www.caida.org/dynamic/analysis/security (analysis of propagation etc)
- www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/
- www.cotse.com “Church of the Swimming Elephant”, (source of attack tools for testing)

.. estimated that only 34% of organisations admit to having been attacked (eg Nimda)

Computer Emergency Response Teams (certs)

- www.apcert.org (Asia-Pacific)
- www.singcert.org.sg (Singapore)
- www.auscert.org.au (Australia)
- www.gcsb.govt.nz/ccip (New Zealand)
- www.hongkong.cert.org (Hong Kong)
- www.mycert.org.my (Malaysia)
- www.certcc.or.kr (Korea)
- www.cncert.org.cn (China)
- www.jpcert.or.jp/english (Japan)
- www.cert.org/advisories (US)

Viruses, Worms and Network Propagation Systems

- Trojan Horses
  - Installing a trojan horse program allows attacker to access user's machine remotely (via Internet)
  - Often received as e-mail attachments
  - Two components: client application, (runs on attacker's computer), and server application, (runs on victim's computer)

Trojan Horse contd …..

- Trojan Horses are distinct from viruses/worms. Do not infect files and have no means of propagation
- A Trojan Horse is program which pretends to be benign, but contains malicious code
- Normally waits to be downloaded or installed by a user - then its attack payload executes

Trojan Horse - Back Orifice 2000 (BO2K)

- Also call Netbus 1.2, 1.53, 1.60, 1.70, 2.0 ….
- Operates on all Windows machines
- Remote attacker can login, send, receive files
- Can re-route and defeat firewall configurations as it can operate on any port
- Very difficult to detect, filename can be made invisible
- Mobile version (Mobile BackOrifice) available
- Other examples include:
  - PKZIP 3, FTP, SubSeven
  - Attack FTP Installer, BackDoor, DeepBO, Executor, FTP99, Happy99

Back Orifice 2000 (BO2K)

- Client machine can monitor and control a server:
  - Execute any application on target machine
  - Log keystrokes from target machine
  - Restart target machine
  - Lockup target machine
  - View contents of any file on target machine
  - Transfer files to and from target machine
  - Display screen saver password of user on target
- Very vulnerable to attack without a firewall!

Other Trojan Horse Programs

- PKZIP 3 Trojan
  - No real v3 PKZIP. This rogue version attempts to reformat the hard drive
  - Works by stealing reputation of another and making download freely available on the Internet
  - It was never available from www.pkware.com
- Wuarchive FTPD Trojan
  - Nasty replacement for the widely used FTP daemon
  - Allows Trojan back door root access and privileged mode access

Other Trojan Horse Programs

- SubSeven Server Trojan
  - Similar to BO2K
  - Machines can be infected by e-mail attachments containing the virus
  - This Trojan was distributed under pretence of being an anti-virus program for detection of non-existent virus
  - Modern versions of this Trojan have ability to command infected SubSeven servers from Internet Relay Chat channels, including initiating Ping flood DOS attacks
  - Anti SubSeven Server is a protection and counter-attack tool

Defence Against Trojan Horses

- Best defence is safe computing practices
- Use signature/checksum programs such as Tripwire (see under Intrusion Detection)
- Trojan Horses can come from unsolicited executable e-mail attachments from recognised senders, (resulting from a virus poaching that person's e-mail address book)

Defence Against Trojan Horses

- Virus-friendly applications, eg Outlook Express will often hide extensions of certain file types
- Famous example AnnaKournikova.jpg.vbs attachment (13/2/01) appearing in Outlook Express to be the much more benign AnnaKournikova.jpg
- Some e-mail programs will even automatically run received attachments to be helpful!!

Evolution of the Threat

Stage III
Mass-Mailers
and Worms

Viruses Gain Complexity. Start to Take Over Machines and Steal Data. No Longer Needs Human Element to Spread

Stage II
"Macro Era"

95 - 98 Virus Numbers Grow Rapidly. Viruses Spread Rapidly e.g. Macro Viruses via E-Mail

Stage I
"Floppy Era"

80's -94 Localised Impact e.g. Michelangelo

The New Trend - Blended Threats

Code Red for example:

- Hacking technique, with propulsion of a worm!
  - No user interaction required
  - No disk infection
  - Code Red sits in memory and sneaks across the Internet on the back of HTTP communications between MS web-servers
- Watch for ‘copy-cat’ variants eg Blaster (August 2003) was a variation on a Windows RPC Buffer Overflow released a month earlier (July 2003)

The New Trend - Blended Threats

- Worms that drop parasitic viruses
- Destructive Trojans
- Password stealers
- RATs (Remote Access Trojans)
- Trojanised applications which replace legitimate system tools
- Multiplatform attacks (payloads affecting multiple platforms), eg Linux worms that drop.exe Trojans

….further blending of worms + viruses + Trojans

Blended Threats - Recent Example

- Bugbear (W32/Bugbear@MM) - Sept 30, 2002
  - Blended threat worm - very nasty!
  - Uses multiple infection paths, disables anti-virus and firewall software, and exploits IE vulnerabilities
  - Can also install backdoor Trojan and key-logger

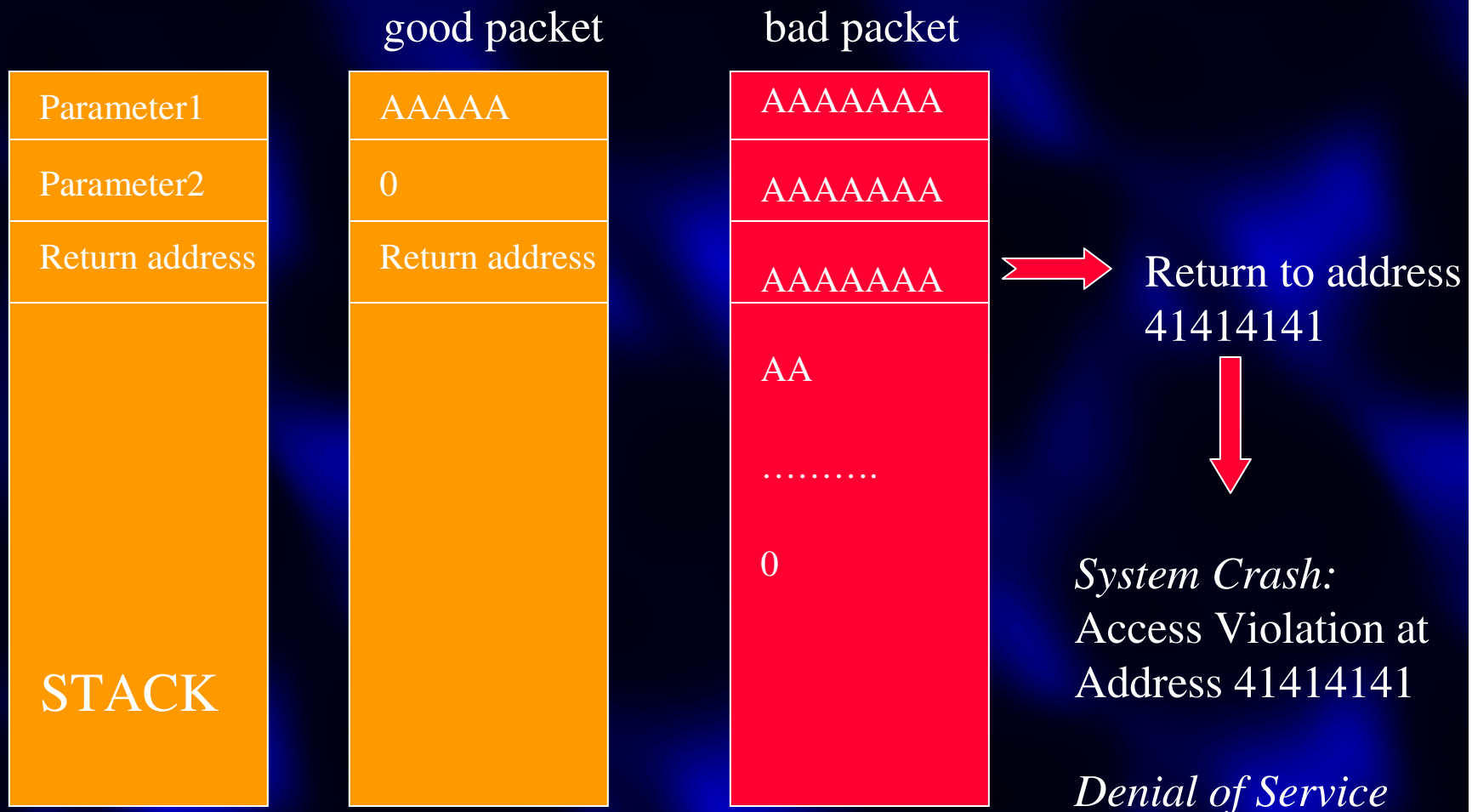
Buffer Overflow - Common Attack Method

- Technique used to gain remote execution on host
- Takes advantage of inadequate vetting of integrity of incoming TCP/IP packets
- Often involves overwriting return addresses on the stack
- Involves sending executable code as binary data within an attack packet, usually carefully crafted to be located at specific position within packet
- May be complicated by the need to encode the packet, eg Base64, uuencode

Buffer Overflow - contd

- Question - Why does an operating system not check for buffer overflows?
- Answer - In many cases it does. For example when a user logs in various checks are made
- The problem occurs when rogue (attack) packets arrive after all checking has been carried out
- Question - why not check every field of every packet everywhere in the system?
- Answer - !!!!!!

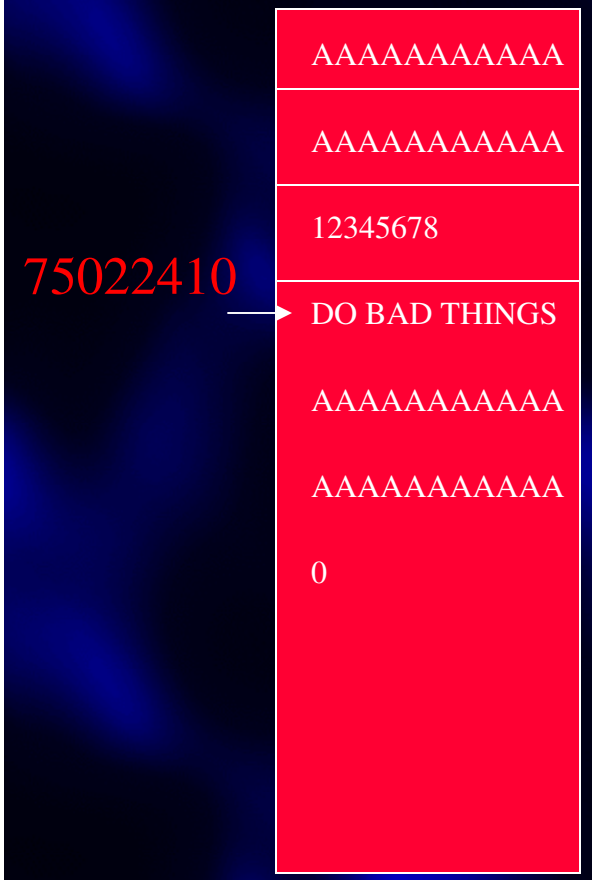
Buffer Overflow - contd



Buffer Overflow - contd

- In previous slide Parameter1 and Parameter2 are fields obtained from (rogue) packet and placed in stack. Parameter1 overflows fields & return address
- The return address becomes X”41414141” which causes a crash = DOS attack
- In following slide an alternative attack causes the return address (12345678) to Call the ECX register which points to some nasty code in the rogue packet
- Either way DOS is achieved
- Common problem with RPC ports where both ends are already trusted and authenticated but rogue packets enter network (eg with spoofed IP addresses - to follow)

Buffer Overflow - contd



Return to address
12345678

EAX	0	
EBX	12345660	
ECX	75022410	

……...		
12345677	NOP	
12345678	CALL	ECX
1234567A	AND	EAX,EAX
……...		

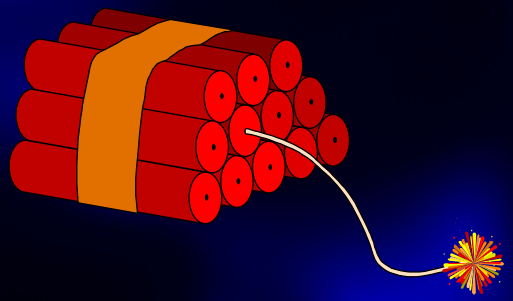
Voila!

Buffer Overflow - contd

- How can this happen if client is authenticated and where both ends are already trusted?
- Rogue packets enter network (eg with spoofed IP address)
- Common problem with RPC ports (for example)

Network Layer Attacks

- IP Spoofing (Masquerading)
- TCP Session Hijacking
- TCP Sequence Number Attack



Threats to TCP/IP

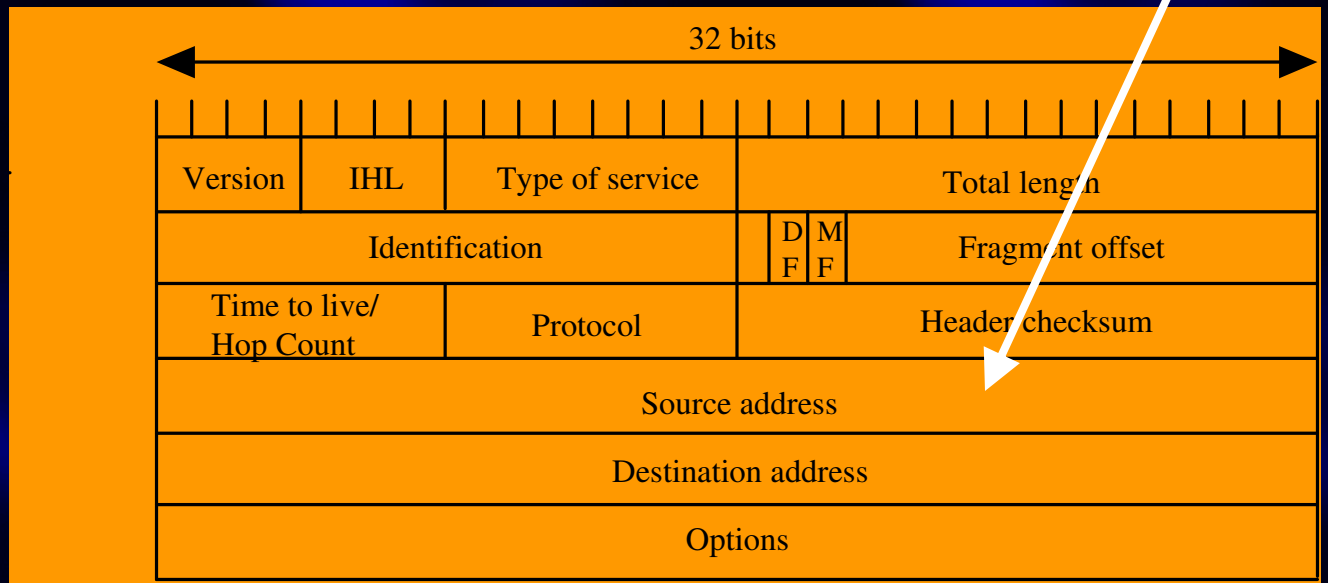
- IP Spoofing
- TCP Sequence Number Attack
- TCP Session Hijacking

Often combined

All exploit weaknesses in TCP/IP and source code freely available on the Internet

IP Spoofing

- IP packet header (Version 4) vulnerable to attack
- Christmas Day attack - source IP address forged
- Source routed packets vulnerable to IP header tampering
- Easy for *internal* attackers

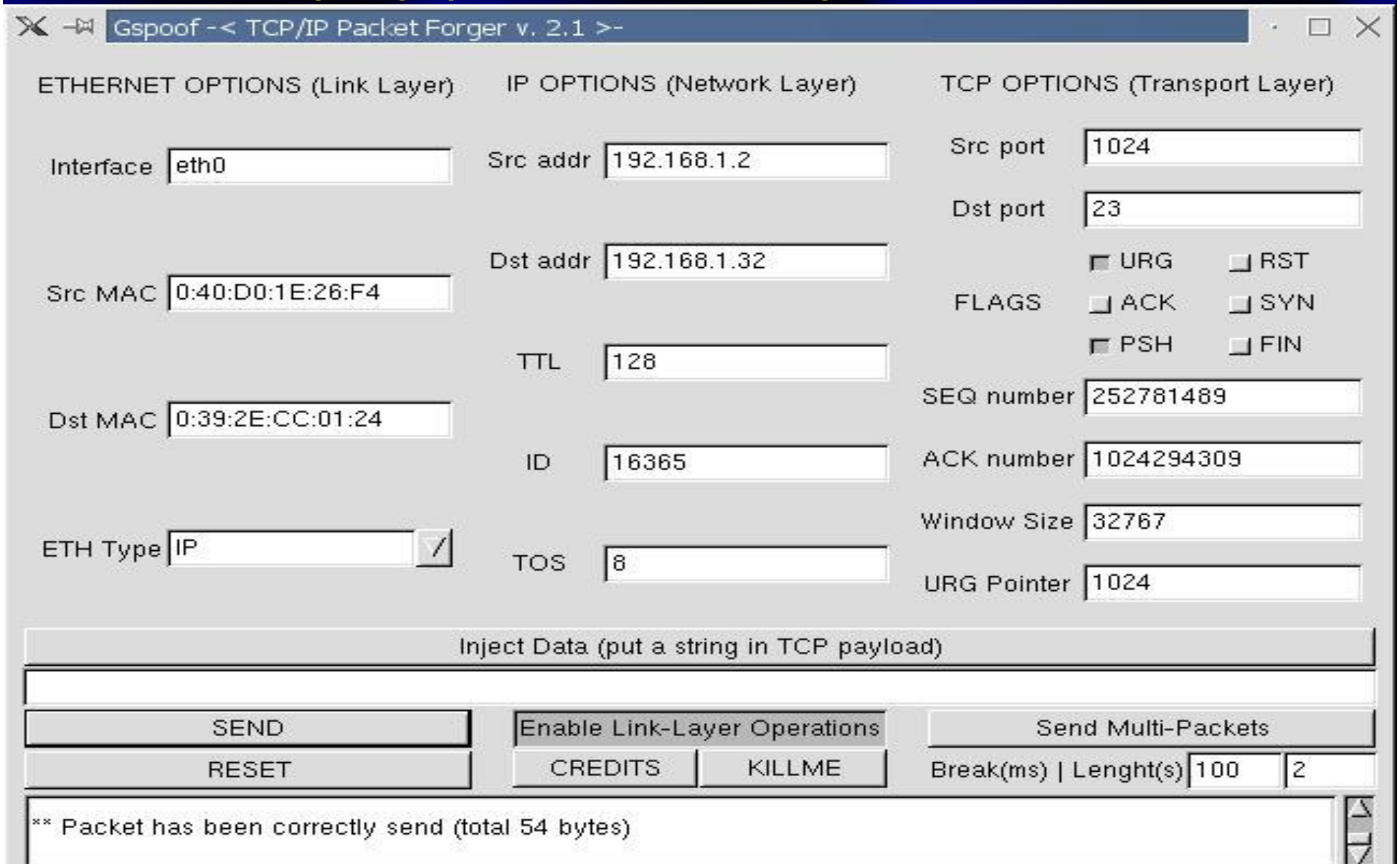


IP Spoofing

- Attacker impersonates host at IP layer by forging source address using RAW-socket. This feature now available in Windows XP!
- Commonly used to launch SYN flood attacks, ICMP redirects, and ping flooding
- Target host has no way of knowing IP address has been spoofed
- DNS spoofing works by returning incorrect address
- IP spoofing combines with TCP seq. number attack …

Spoofing an IP Packet

Ref: http://gsproof.sourceforge.net/screenshots



Threats to TCP/IP

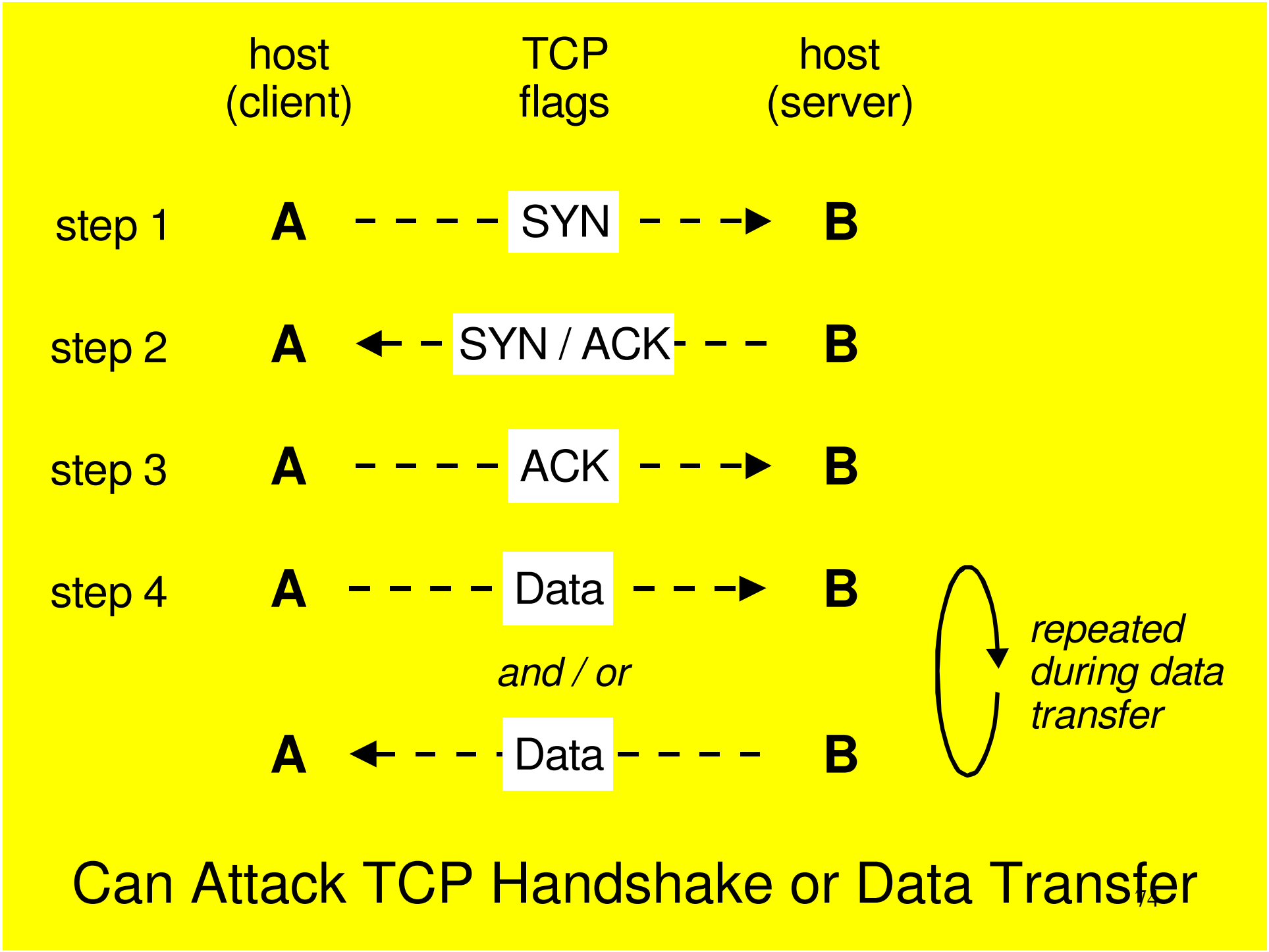
- IP Spoofing
- TCP Sequence Number Attack
- TCP Session Hijacking

Often combined

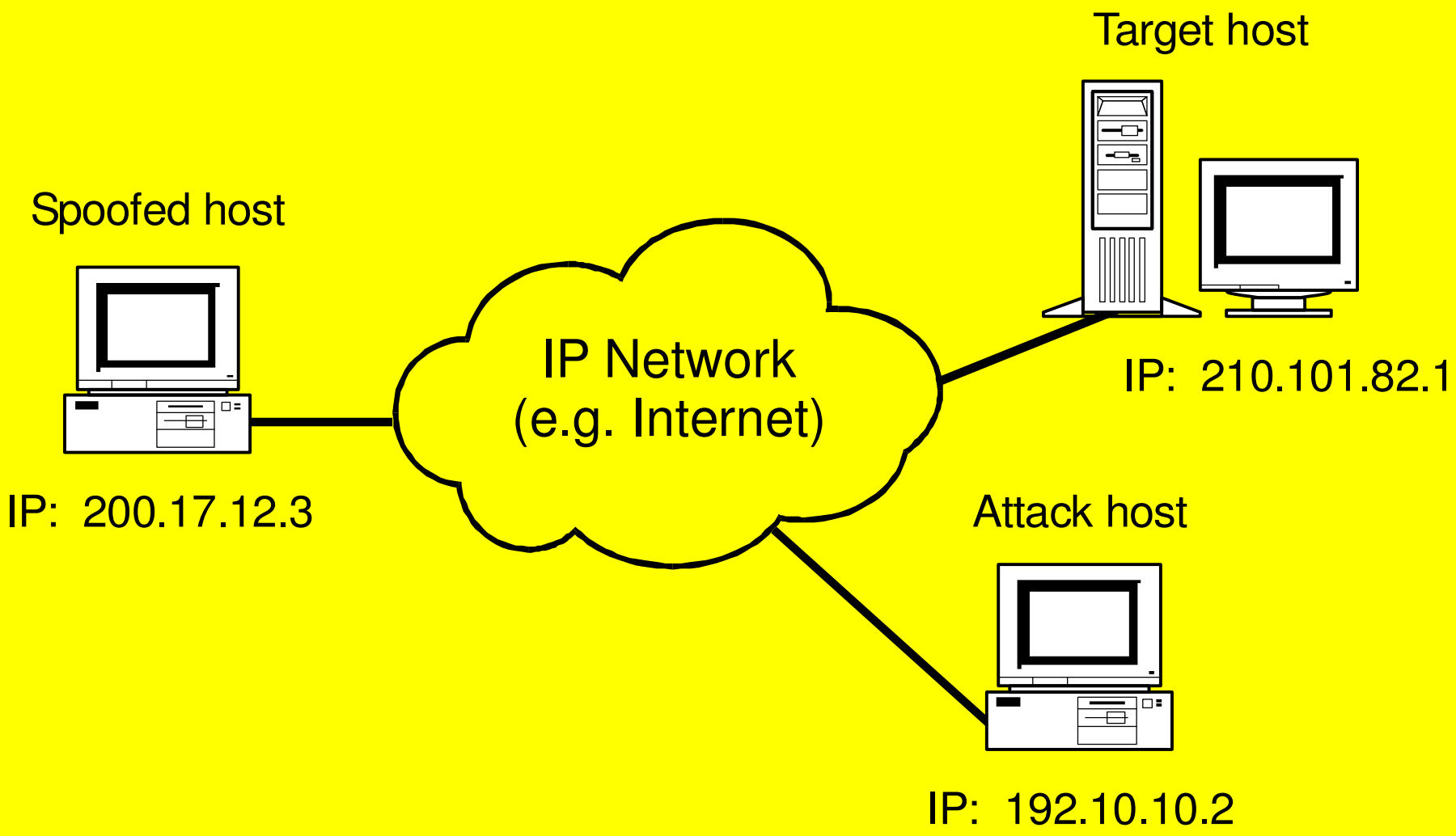
All exploit weaknesses in TCP/IP and source code freely available on the Internet

TCP Sequence Number Attack

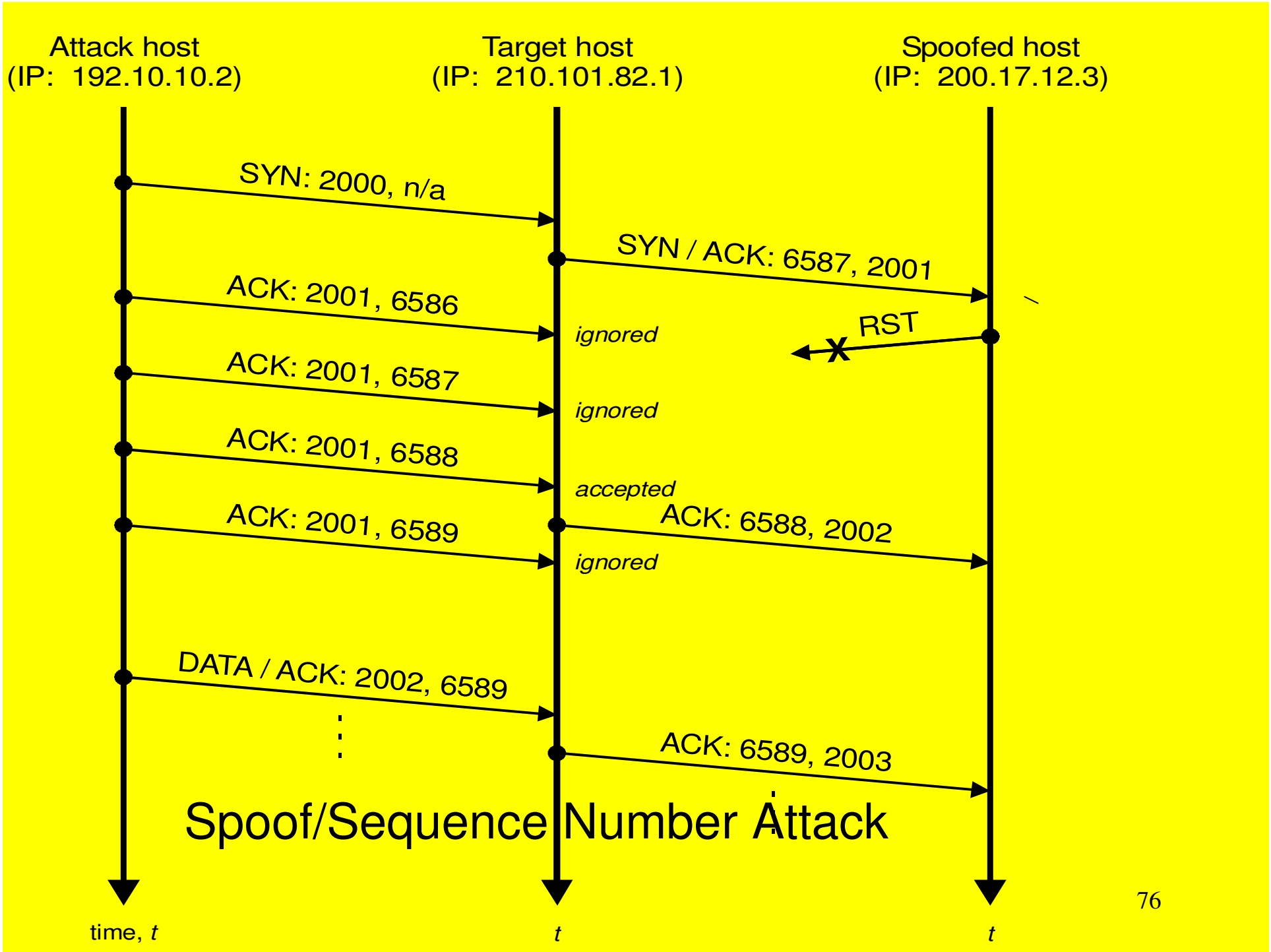
- TCP sequence number prediction takes advantage of TCP's sequenced data delivery
- If attacker determines correct sequence number then they can generate own TCP segments
- Two methods:
  - attack TCP handshake (TCP (IP) spoofing)
  - take over legitimate session (TCP hijacking)



Can Attack TCP Handshake or Data Transfer



Spoof/Sequence Number Attack


Attack host
(IP: 192.10.10.2)
Target host
(IP: 210.101.82.1)
Spoofed host
(IP: 200.17.12.3)
SYN: 2000, n/a
SYN / ACK: 6587, 2001
ACK: 2001, 6586
ignored
RST
ACK: 2001, 6587
ignored
ACK: 2001, 6588
accepted
ACK: 2001, 6589
ACK: 6588, 2002
ignored
DATA / ACK: 2002, 6589
ACK: 6589, 2003
Spoof/Sequence Number Attack
time, t
t
t

TCP Sequence Number Attack

- Attacker must ensure spoofed host is unreachable, otherwise it will receive SYN/ACK and issue RST to defeat attack
- Attacker must therefore
  1. wait until spoofed host off-line or
  2. take it offline with denial of service attack (eg SYN flood)
- Non-Blind Spoofing
  - easy - attacker on same LAN segment as target host
  - can use protocol analyser for direct access to IP packets and TCP sequence numbers

TCP Sequence Number Attack

- Blind Spoofing
  - attacker on different LAN segment from target host
  - must guess initial TCP sequence number based upon operating system. Three ways -

  1. 64K rule - used in older OSs (eg OSF, SunOS)
  2. time related generation of sequence numbers
  3. pseudo-random generation of sequence numbers

  - prediction almost impossible with 2 and 3

TCP Sequence Number Attack

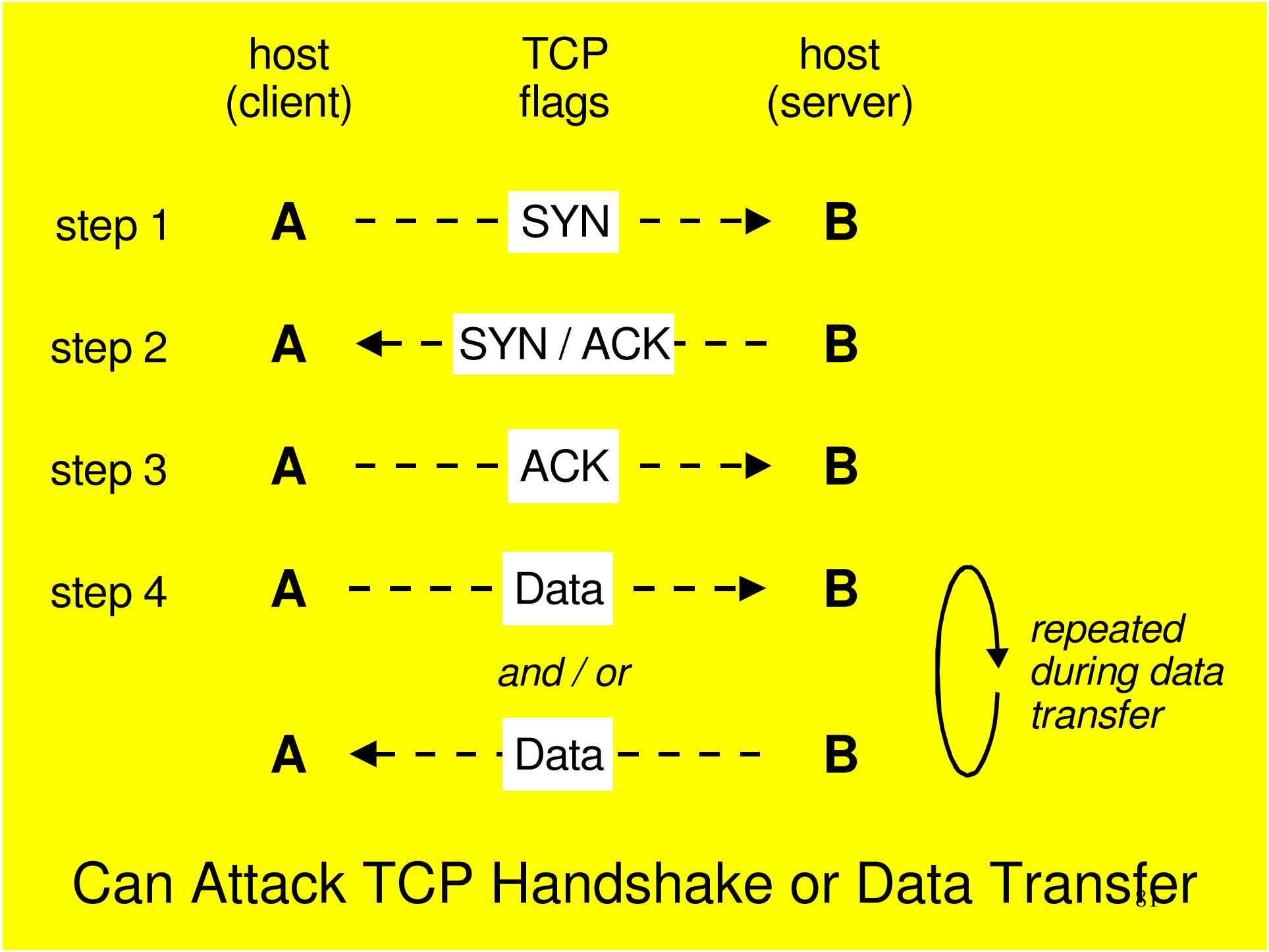
- Blind Spoof can be turned into Non-blind Spoof by using source routed IP packets or affecting routing tables en route
- Source routed packets allow return route to be specified in IP packet header which can be spoofed by attacker
- Therefore very important to drop source routed IP packets - especially if they originate from an untrusted network

Threats to TCP/IP

- IP Spoofing
- TCP Sequence Number Attack
- TCP Session Hijacking

Often combined

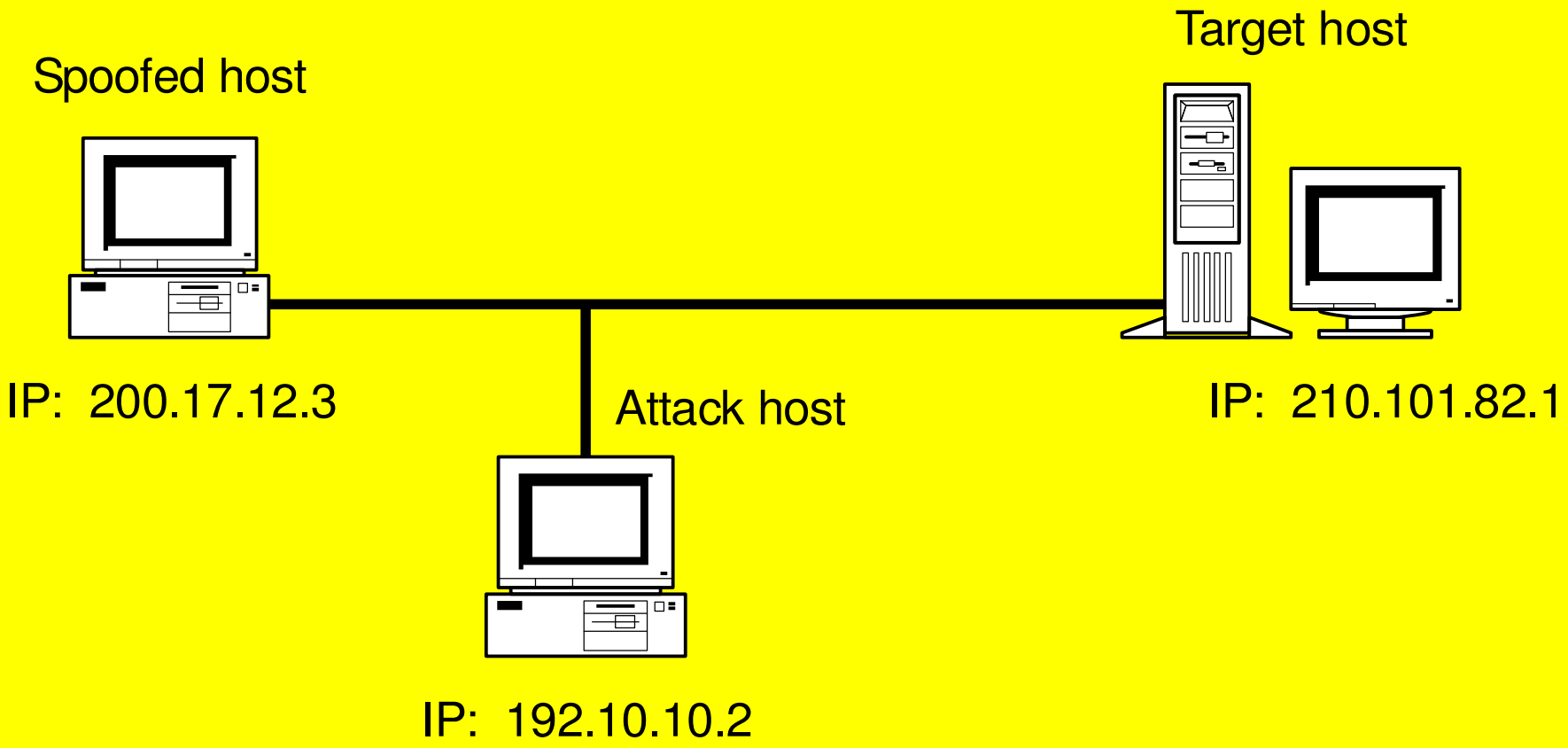
All exploit weaknesses in TCP/IP and source code freely available on the Internet



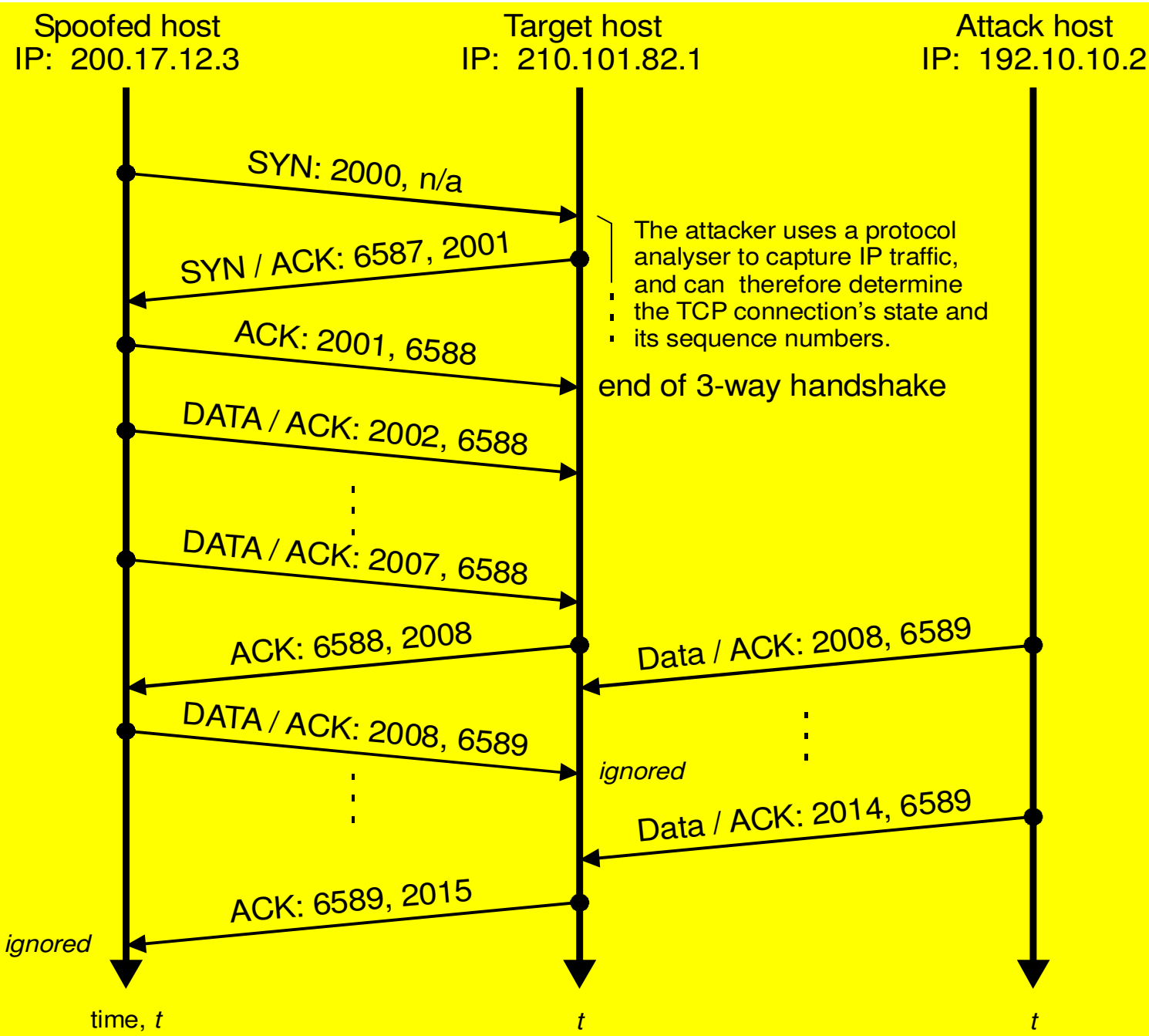
Can Attack TCP Handshake or Data Transfer

TCP Session Hijacking

- TCP session hijacking used in conjunction with IP spoofing and TCP sequence number attack
- Can be used to take over TCP applications like Telnet, FTP, rlogin
- Once attacker has TCP segment sequence they can take over connection
- All packets then sent by hijacked (spoofed) host will be ignored by target host as sequence numbers will be incorrect



TCP Session Hijacking



TCP Session Hijacking

TCP Session Hijacking – counter-measures

- TCP session hijacking can circumvent one-time passwords and is smarter than simple sniffing
- ISPs can help by blocking all IP packets with source addresses which originate from outside the domain (spoofed addresses)
- Trusted hosts (eg .rhosts) should only be used with authentication and encryption
- Correctly configure firewall

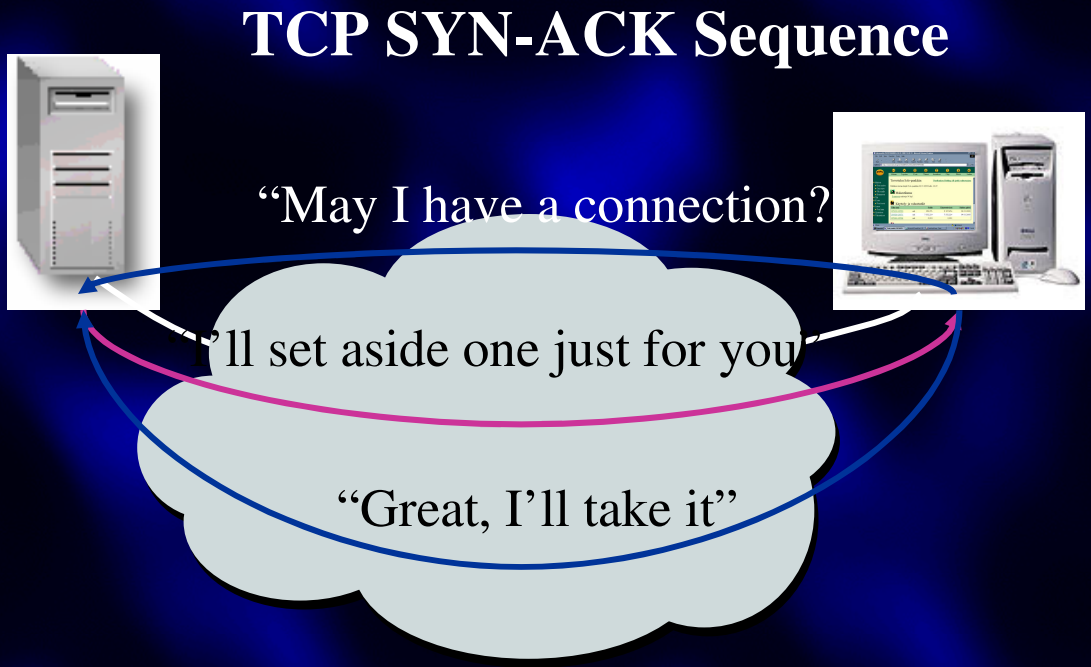
Denial of Service Attacks

- Intention is not to gain illegal access but to make network services unavailable to users
- Sometimes called *nuke* attack
- Flooding attacks overload server
- Examples include: - Ping o' Death, SYN Flood, ICMP redirect messages
- No real solution but sharing services across different servers and using a properly configured firewall can assist

(Distributed) Denial of Service Attacks

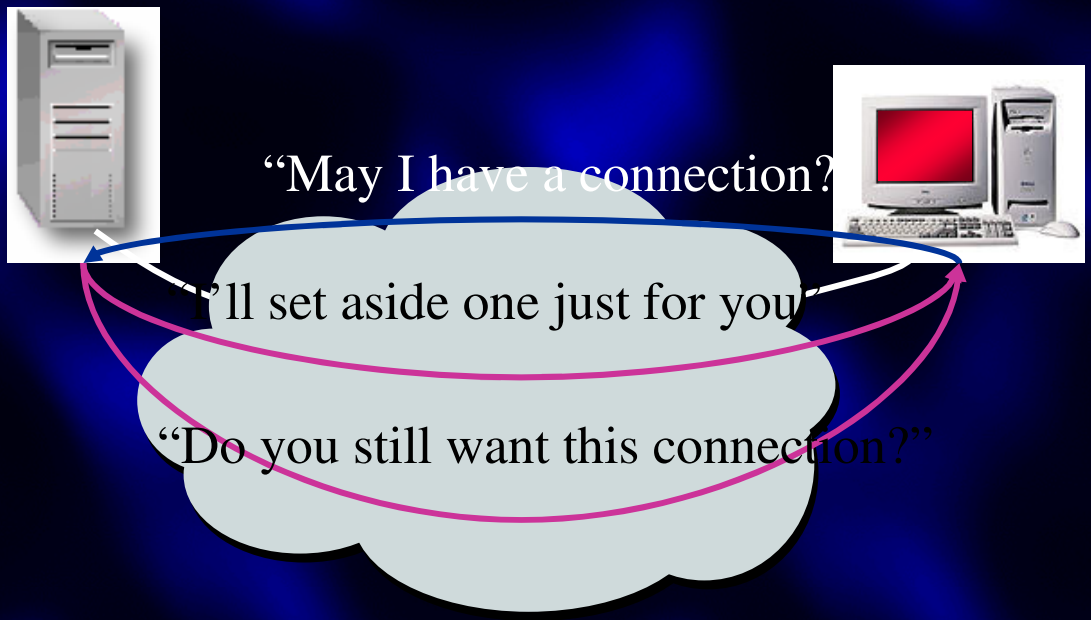
- Distributed DOS attack requires co-ordination from multiple sites
- Two categories:
  - Operating System Attacks - exploit known weakness and vulnerabilities
  - Network Attacks - exploit limitations of network resources, eg flooding
- http://packetstormsecurity.org has plenty of attack tools available for download!!

Normal TCP Connection Set-up



Abnormal TCP Connection Set-up

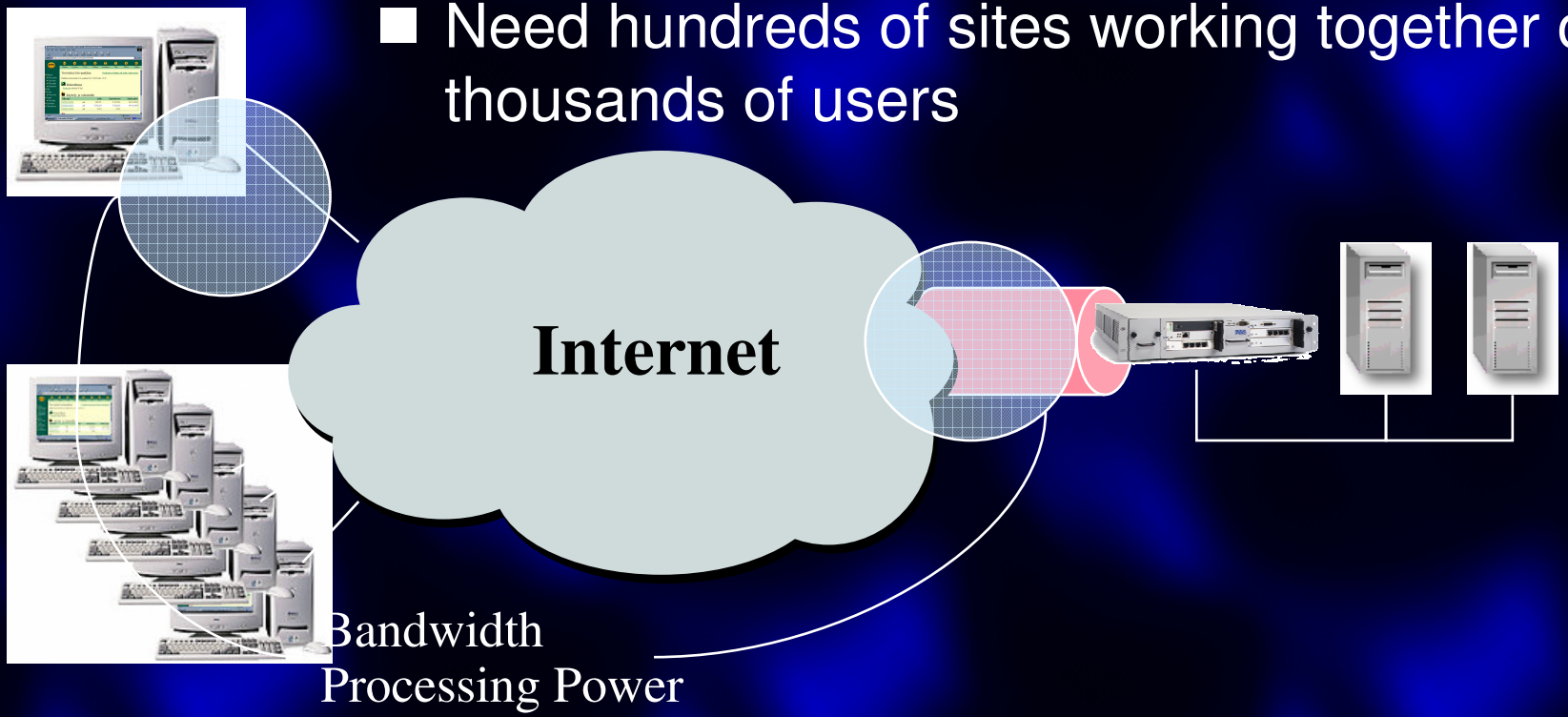
TCP SYN-ACK Sequence



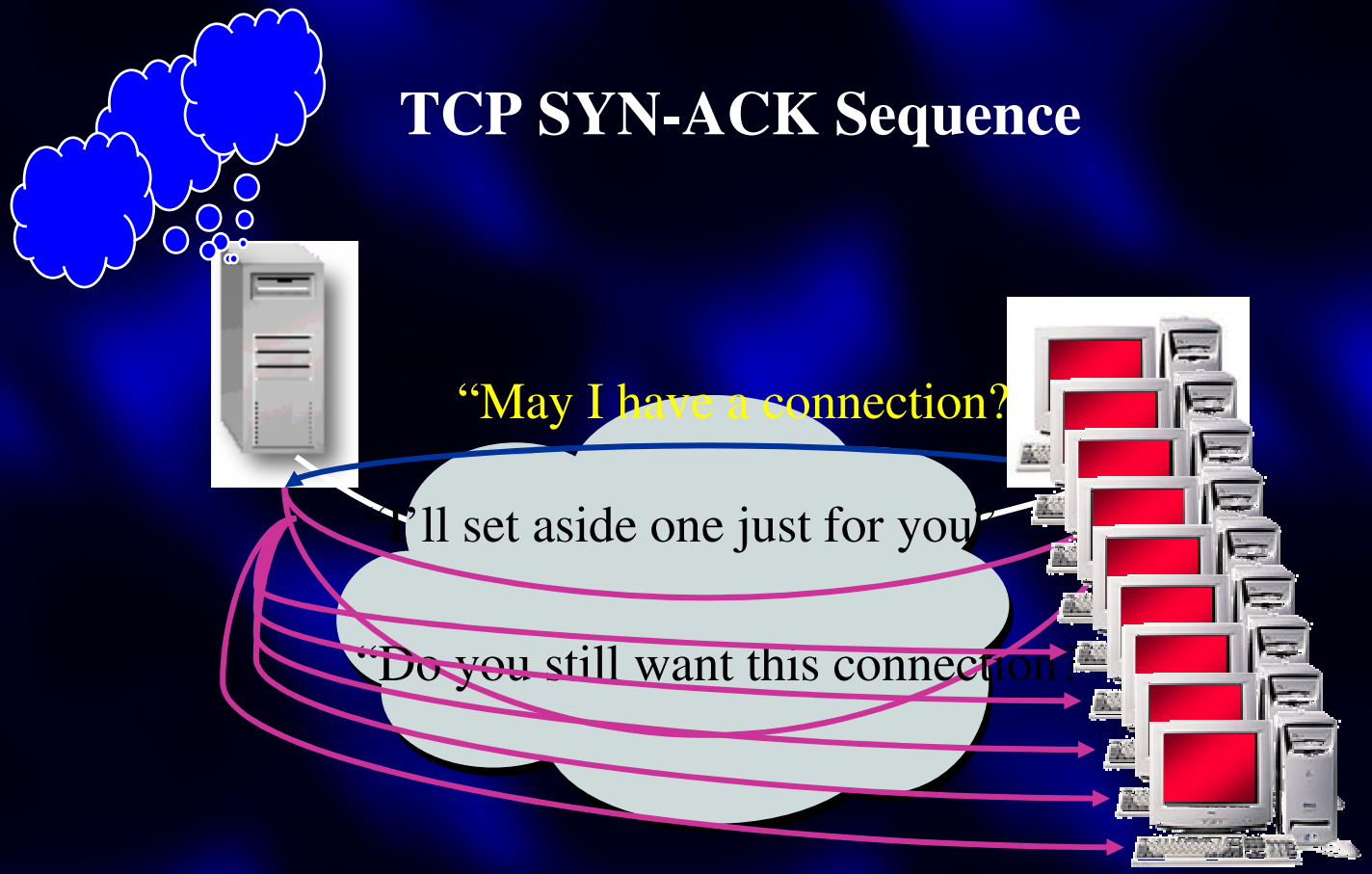
- Connection Setup Incomplete

Bringing a major web site to its knees

- More than a lone user on a modem
- Need hundreds of sites working together or thousands of users



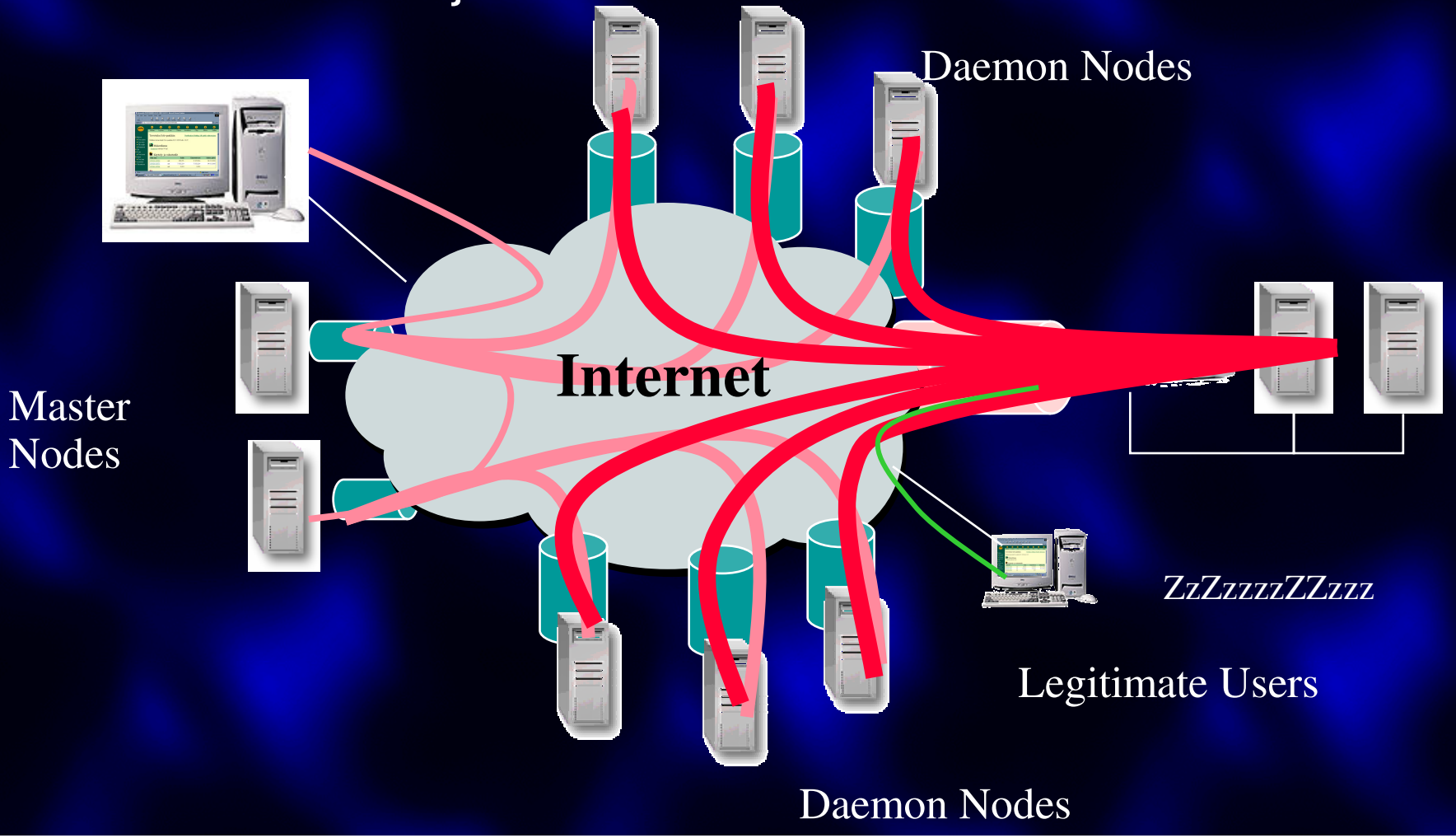
Organised DOS Attack



- Over time, other requests will not be serviced
- System locks up, does not really die - just impaired

Distributed DOS Attack

- Multiple users are difficult to co-ordinate and can be traced
- Better to use hijack intermediate sites



DOS Attack Classification

- Operating System Attacks
  - ActiveX/Pentium III
  - Bonk/Boink
  - Jolt
  - Land
  - NestEA
  - NT inetinfo
  - NT MsgBox
  - NT Stop
  - Oshare
  - Out of Band (OOB)
  - Ping of Death
  - Snork
  - Tear Drop
  - Win/Arp/Poink

Ping o' Death DOS Attack

- Tests for host by using ICMP packet
- Ping data payload can be 64K bytes
- Possible to create (offset + size) > 64K
- ping -l 65510 (buffer size) ip# will launch attack
- This can cause overflows, system crashes, reboots, kernel dumps etc
- Patched in most systems
- Block fragmented pings (eg 64-byte pings only)

Tear Drop Attack

- Attacker sends overlapping packets to victim
- When victim machine attempts to re-construct packets it hangs
- Bonk Attack does same thing by sending corrupted UDP packets to port 53 (DNS)
- Affects unpatched machines

Land Attack

- Attacker sends spoofed packet(s) with the SYN flag set to any open port that is listening on victim's machine
- Packet(s) contain same destination and source IP address as the host
- Victim's machine hangs or reboots
- Systems can freeze, where CTL-ALT-DEL fails to work, mouse and keyboard become non-operational

Other OS-based DOS Attacks

- Snork
  - overload of CPU with continuous bounce attack
- WinArp/Poink
  - overload with spoofed ARP packets
- NT Stop
  - invalid SMB block size
- ActiveX/Pentium III
  - hostile code in web pages causing the “Blue screen of death”
- Jolt
  - spoofed and fragmented ICMP packets which cannot be reassembled

DOS Attack Classification

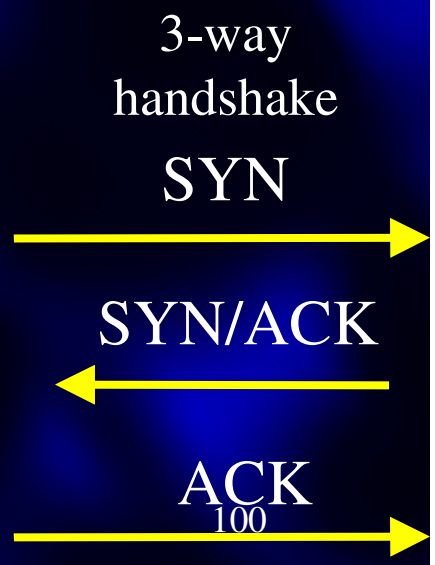
- Network Attacks
  - Click
  - Coke
  - Smack/Bloop
  - Smurf
  - SYN Floods
  - TCP FIN/RST bit
  - Winfreez
  - +++ATHZero

Smurf Attack

- ICMP echo (pings) sent to broadcast addresses
- Source address is spoofed and is that of the victim
- Potentially every host can reply to each broadcast
- For *n* hosts and *m* broadcasts then victim receives *n x m* responses

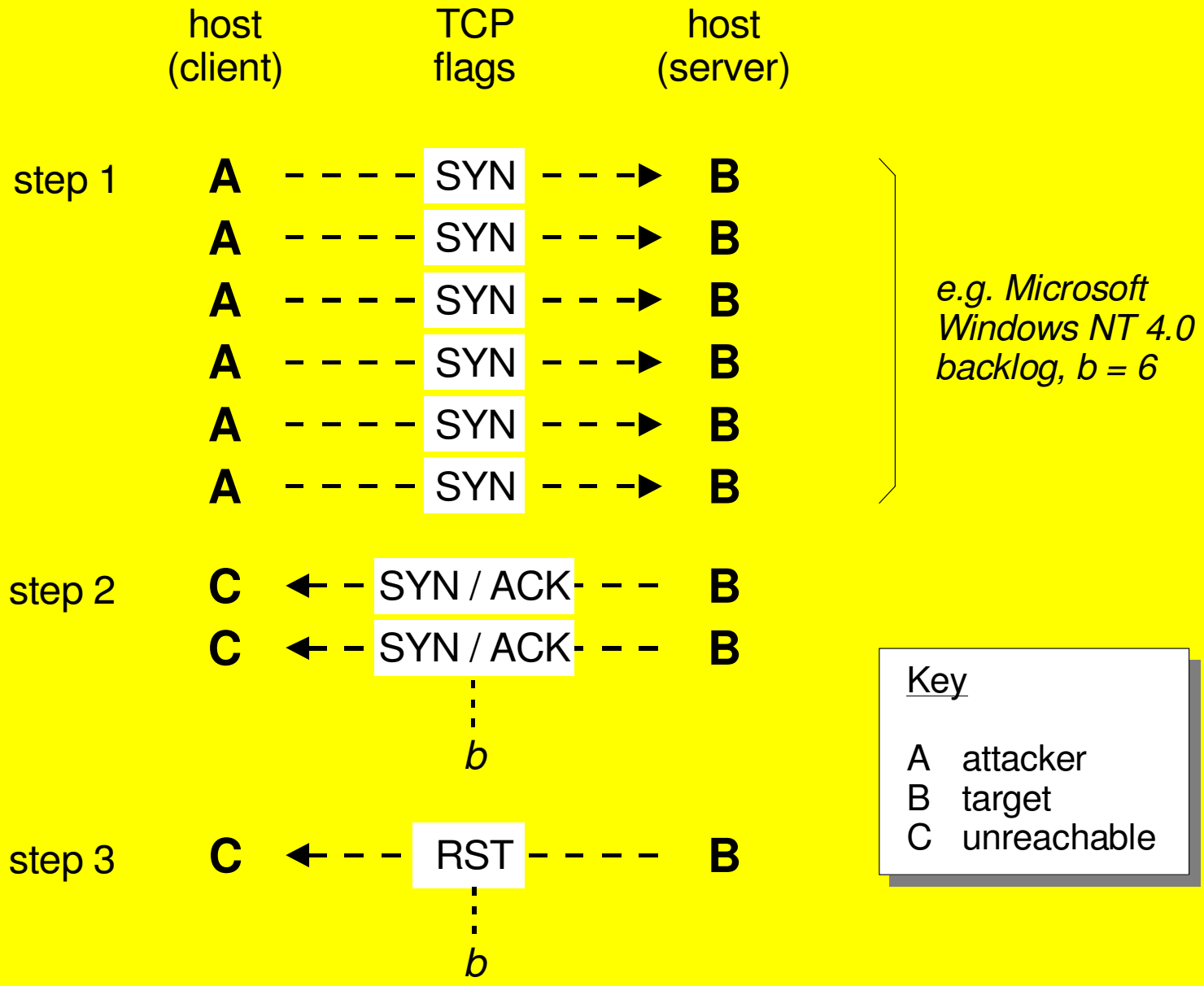
SYN Flooding

- Server receives more incomplete connection requests than it can handle
- Source code published on Internet
- Prevents completion of 3-way TCP handshake by withholding ACK flag



SYN Flooding

- Number of half open connections limited
- Server rejects subsequent requests until existing requests time out $\rightarrow$ 75 secs creating denial of service
- Attacking host must spoof source IP address to routable but unreachable host
- Randomisation of (unreachable) source address assists in hiding attacker's location



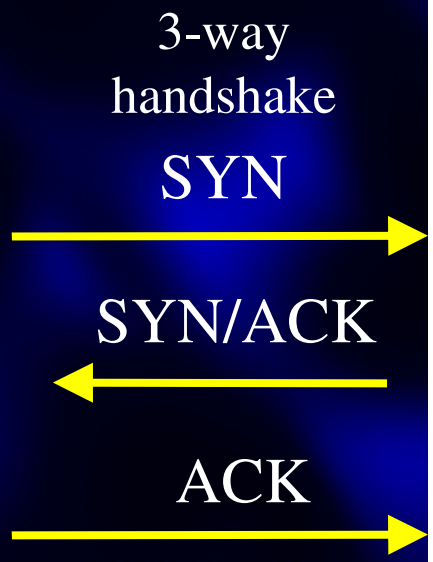
TCP SYN Flood Attack

SYN Flooding – counter-measures

- ISPs can block IP packets with non-internal addresses from reaching the Internet
- Intrusion detection tools
- Modifications to operating system - eg increase size of backlog queue, randomly drop half-open connections

TCP RST and FIN DOS Attacks

- TCP - control flags for segment status
- RST (resets connection) and FIN (finish of data) can be used for DOS attacks
- If RST or FIN contain correct sequence # they will be accepted (no ACK reqd)
- Protocol analyser used to determine sequence numbers between spoofed and target hosts



TCP RST and FIN DOS Attacks

- Generate TCP segment with RST flag set + correct sequence number and placed in spoofed IP packet then connection closed
- FIN flag can be used in same way
- Any further TCP segments sent from spoofed to target host are ignored
- RST and FIN attacks only possible on internal TCP networks

Other Network-based DOS Attacks

- Coke
  - garbage attack on WINS - fills the log!
- Click
  - Flood with ICMP unreachable error messages causing connection termination
- Smack/Bloop
  - Similar to Click but without connection termination
- Winfreez
  - Spoofed ICMP packets causing routing table corruption
- +++ATHZero
  - attack to terminate connection to Hayes modem

Some DDOS Tools

- Trin00 (Trinity 2000)
  - co-ordinated UDP flood attacks from multiple sources
- TFN (Tribal Flood Network)
  - similar to Trin00 but can also launch TCP SYN flood, ICMP echo request and ICMP broadcast attacks
- Stachedraht [= barb wire in German]
  - combines features of Trin00 + TFN + encryption of traffic between attacker, masters and agents components)
- TFN2K (Windows + UNIX are vulnerable)
  - combination of above with more sophisticated features

Case Studies of DOS Attacks

- eBay, Amazon, CNN, Yahoo, E*Trade, all hit 7-11Feb 2000 - up to three hours of sustained attack and sites unreachable
- DOS attack on *all* Cisco Router IOSs (July 2003). Critical attack blocking *all* traffic on *all* routers
- Major impact for those companies who depend on the network for their livelihood

Preventing DOS Attacks

- DOS attacks are very difficult to prevent
- Important that DOS staging points not available
- DOS attack S/W available on the Internet - much of it has sophisticated capabilities and thousands of launching sites may be harnessed
- Tools can completely remove themselves and provide cover
- Encryption is used between components to prevent detection (Stachedraht + TFN2K)

Preventing DOS Attacks

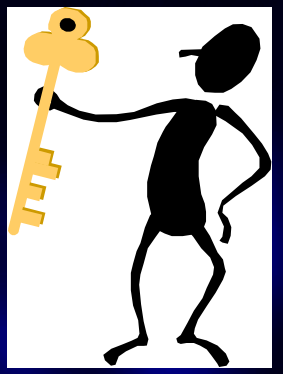
- Secure all servers
  - protects against attack and as a relay point
- Distribute load across multiple servers
- Machines with E1/E3 and other high speed access are at high risk
- Good packet filtering at firewall
- Disable Directed Broadcasts
  - protects against Smurf attacks
- Get ISP to implement ingress filtering services

Some Specific DOS Attack Prevention Measures

- Configure gateway routers for *egress filtering* - prevents spoofed traffic from exiting network
- Use firewall with application proxies, which should block all TFN2K traffic + *new tracking methods*
- Disallow unnecessary ICMP, TCP, and UDP traffic
- Disallow UDP and TCP except on a specific ports
- Remain current with security-related patches to operating systems and applications software
- Regularly scan network file systems for evidence of infection by DOS tools

Threats to TCP/IP Services

- Simple Mail Transport Protocol (SMTP)
- Telnet
- Network Time Protocol (NTP)
- Finger/Whois
- Network File System (NFS)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- ActiveX
- Secure Shell (SSH)
- Domain Name Service (DNS)
- NetBIOS
- Server Message Block (SMB)



Simple Mail Transport Protocol (SMTP) - Port 25

- E-mail is most popular Internet application
- Original problems centred on sendmail and Internet worm and……..
- Denial of Service Threats:
  - E-mail flooding
  - Large messages or attachments (>1 Mbyte)
- Information Gathering:
  - VRFY command can translate mail alias to login
  - CRACK can then be used

SMTP - Port 25 … Case Study

- Some recent statistics relating to SoBig.F (August 2003). Organisation X
- Filters for:
  - Unsafe attachments
  - Viruses

  } → 80K per day dumped = 1 per second (24 x 7)

  - Blackhole List → 20-40K per day dumped
- PreciseMail Anti-Spam Gateway had a discard rate of over 50% of all e-mail (cf AOL statistics of 57% during peak of SoBig.F)

You must pay for the mail you don't want!

SMTP - Port 25 contd ….

- Spam and Mail Relay Attacks
  - PreciseMail Anti-Spam Gateway (SoBig.F) (www.process.com/precisemail/precisemailds.htm)
  - SpamAssassin (http://spamassassin.org)
  - MailMarshal and WebMarshal (www.marshalsoftware.com)
  - GFI Mail Security (www.mailessentials.com)
  - Spam Tester (www.dnsstuff.com)
  - Mail abuse prevention system (www.mail-abuse.org)

SMTP - Port 25 contd ….

- Additional filters for junk mail include:
  - RBL - Realtime Blackhole List - addresses of ISPs who are know to be sources of spam mail
  - DUL - Dailup User List - addresses of spammers who attempt direct connection to mail servers rather than using ISPs mail server
  - RSS - Relay Spam Stopper - addresses of ISPs who allow themselves to be used as a mail relay

SMTP - Port 25 contd ….

- Spam and Mail Relay Attacks
  - Firewall proxy needs to be configured to:
    - (allowed to:) block incoming traffic posing as an insider, eg administrator@silverfire.com coming from outside
    - (denied from:) block outgoing access where source is not ……@silverfire.com (relaying spam mail)

SMTP - Port 25 contd ….

- Question…..
- Suppose that the manager wants to be a roaming client. How can they be provided with access?
  - Build a tunnel and use PPTP/IPSec encryption allocating an IP number from the firewall for the internal network
  - Set up the “allowed to” and “denied from” proxy rules as discussed - which will block the manager!!
  - Set up another rule which allows access to the e-mail server from a specified IP address (managers PC)
  - Question - which rule takes precedence?
  - Does the second rule override the first?

Telnet - Port 23

- Simple and widely used host independent character-based terminal access protocol
- Threats:
  - ID and password capture during login
  - Packet sniffer can easily detect Telnet session
  - Telnet program itself can be compromised to record IDs and passwords
- Some secure versions of Telnet encrypt passwords and message contents

Network Time Protocol (NTP) - Port 123

- Used to synchronise host clocks on the Internet
- Threats:
  - Altering clocks
  - If successful this can affect a time-based authentication protocol by enabling replaying of previous successful authentication sequences
  - Can confuse time-based backups
- Newer versions of NTP provide cryptographic message authentication and/or control time off-sets (Version 3)

Finger and Whois - Ports 79 & 43

- Provides information on host users (account names, login audit, signature file etc)
- Threats:
  - Can be used to collect useful information on account names, login profiles etc
  - Can provide valuable information for use with CRACK
  - Finger Bomb can be used for Denial of Service attacks, eg finger username@@@@@@hostA (recursive)
  - Finger chaining, eg finger username@hosta@hostb
- Newer versions of finger fix some problems

Network File System (NFS) - Port 111 (Sun RPC)

- Provides transparent remote access to shared files across network and portability achieved with RPCs
- Threats:
  - Files and directories are identified by unique strings - “handles”. Attacker may get root file handle
  - Attacker can then change access controls
  - Trapdoor programs can then be planted
- Encryption and authentication are necessary

File Transfer Protocol (FTP) - Ports 20 (data) and 21 (control)

- Very useful binary and character-based file transfer protocol used on most architectures
- Threats:
  - Like Telnet, FTP does not encrypt IDs and passwords
  - Running public (anonymous) FTP services
  - If access controls are circumvented then file permissions can be changed, trapdoors inserted etc
  - Can be combined with IP spoofing to create “FTP Bounce Attack”
- Mandates careful use of file permissions as well as encryption and authentication

Hypertext Transfer Protocol (HTTP) - Port 80

- Four categories of web security threats:
  - alteration of web site data - weakly secured web servers can be compromised by attackers and the web site data defaced or destroyed (US Air Force, CIA, Justice Dept, Universal Studios)
  - access to web server OS - malicious code can cause buffer overflow and exceptional conditions which give access to the OS. Commands can be embedded in web requests which in turn pass to the OS
  - eavesdropping on browser-server traffic
  - impersonation of another web server (see DNS)

Hypertext Transfer Protocol (HTTP) - Port 80

- Use of Secure-HTTP (SHTTP) in conjunction with SSL/TLS allows client-servers to negotiate security levels for particular transactions
- Most ActiveX and Java applets can be digitally signed (digital certificate)
- Recent versions of browsers ensure that Java and ActiveX executables have no access to system resources

Active X and Java Applets

- Can pass harmful programs across network and execute them through user's browser
- These attacks differ from other application-layer attacks in two main respects:
  - They are initiated not by the attacker but by the user via web page request
  - Attacks are not restricted to specific hardware platforms and operating systems because of software portability

Domains Name Server (DNS) - Port 53

- Potential for DNS attacks are great, but rare
- DNS system is vulnerable to DOS attacks
- Mirroring DNS sites increases functionality but also vulnerability to spoofing attacks
- DNSSEC (DNS Secure) - extension of DNS, prevents spoofing attacks by allowing web-sites to verify their domain names and IP addresses using digital signatures and public-key encryption

Server Message Block (SMB) - Ports 137, 138, 139

- SMB provides file read/write and service requests in Microsoft windows networks
- Clients connect to servers via NetBIOS over TCP/IP
- Clients can send commands (SMBs) to the server that allow them to look up names, access shares, open files, read and write files over the network!!
- This multi-port, multi-protocol service rule opens:
  - port 137 (UDP) for nbname service
  - port 138 (UDP) for nbdatagram service
  - port 139 (TCP) for nbsession service
- For secure configuration, SMB operates over a VPN

Summary

- TCP/IP networks are vulnerable to a wide range of attacks - from password sniffing to denial of service
- Most attack software can be downloaded from the Internet
- Essential to understand common attack methods - SYN Flooding, IP Spoofing, Denial of Service, TCP Session Hijacking etc
- A properly configured firewall with both TCP/UDP/IP port and application filtering is essential
- Cryptographic, authentication and certification services are becoming mandatory