# Network Security: The Principles of Threats, Attacks and Intrusions

APRICOT Tutorial
Perth Australia
28 February, 2006

Danny McPherson, Arbor Networks
Ray Hunt, Associate Professor
University of Canterbury, New Zealand

1

# Agenda

- 9.00 - 9.15: APNIC Presentation
- 9.15 – 10.30: Danny McPherson
- 10.30 -11.00: Morning Tea
- 11.00 - 12.15: Ray Hunt
- 12.15 – 12.30: Round up and discussion

2


# 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 (Malware)*
  - Network Layer Attacks - spoofing, hijacking
  - Web-based attacks
  - (Distributed) Denial of Service Attacks
- Threats to TCP/IP Application Services

## 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

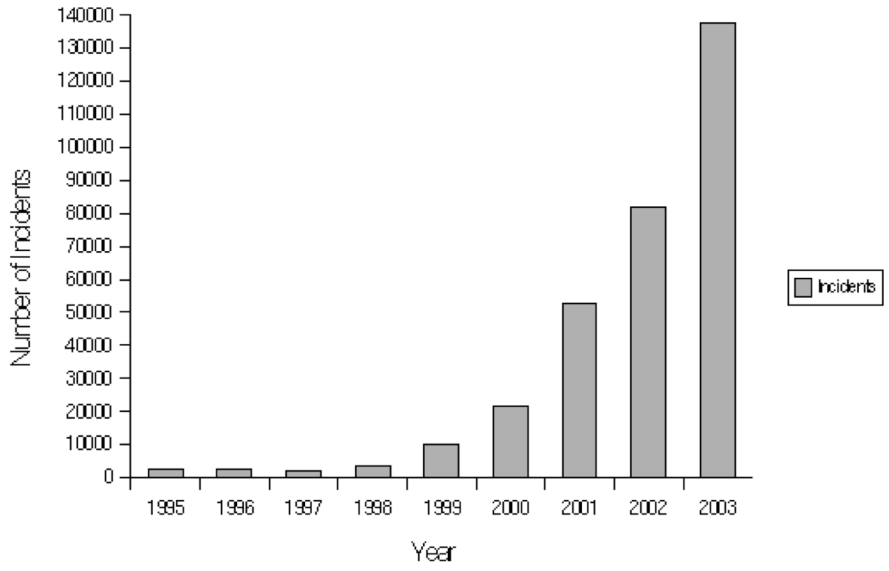
5

## Factors Affecting Attack Trend

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

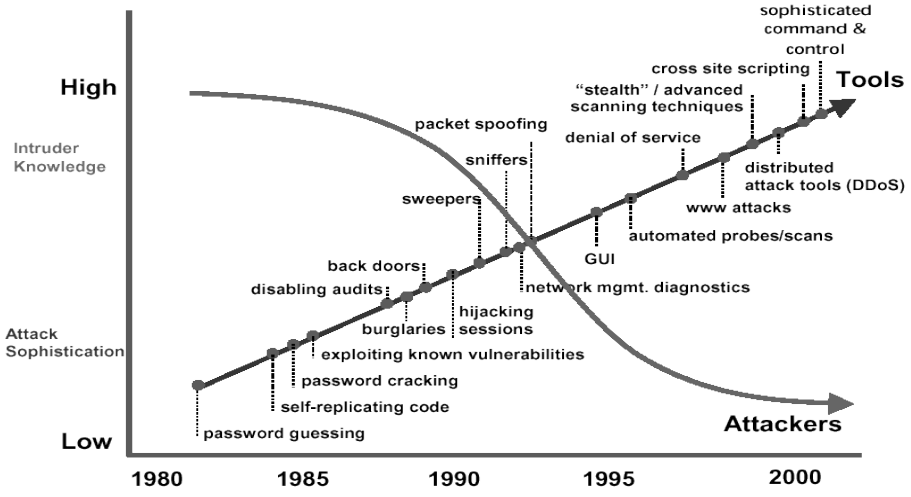
6

# 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

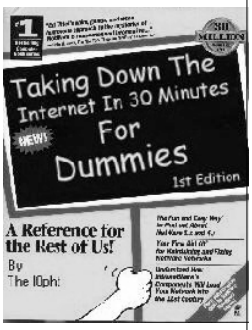
# Main Techniques Used in Attacks

- Port-based attacks
  - eg Slammer, Blaster, ……
- Malicious e-mail attacks
  - eg So Big, MyDoom, Melissa……
- Buffer overflow attacks
  - eg Slammer, Blaster, ……
- Malicious web-based attacks
  - eg Nimda, CodeRed, ……
- (Distributed) Denial of Service Attacks
  - eg TCP Flood, Reflection, Shrew, TFN2K

9

# Classification of Attack Methods

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



## Classification of Attack Methods

- Network Layer Attacks
  - IP spoofing (masquerading)
  - Sequence number prediction
  - TCP hijacking
- Web-based Attacks
  - Cross Site Scripting
  - Cookie Poisoning
  - SQL Injection
  - etc….

## 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 ….
  - Distributed DOS (DDOS) attacks
    - TCP Flood, Reflection, TFN, TFN2K….
  - Preventing DOS attacks

# Social Engineering

- Persuade someone to disclose sensitive information (eg Phishing attacks on bank customers, etc)
- Persuade someone to run/install malicious or subverted software
- Invite someone to log into a bogus web site such as a spoofed bank web site
- Impersonating new employee who has forgotten userid/password
- Impersonating a technical support staff member and requesting a user login to ‘check’ accounts

# Social Engineering - Phishing

- Phishing (electronic fishing) attacks - mass distribution of 'spoofed' e-mail
- Appears to come from banks, insurance agencies, retailers or credit card companies
- Fraudulent messages designed to fool recipients into divulging personal authentication data - account usernames / passwords, credit card numbers etc
- Because these emails look “official”, up to 5% of recipients may respond, resulting in financial losses, theft etc

14

## Phishing Attack – Recent Example

**Westpac** Australia's First Bank

Dear client of the Westpac Bank,

The recent cases of fraudulent use of clients accounts forced the Technical services of the bank to update the software. We regret to acknowledge, that some data on users accounts could be lost. The administration kindly asks you to follow the reference given below and to sign in to your online banking account:

https://olb.westpac.com.au/ib/default.asp

We are grateful for your cooperation.



## Phishing Attack - Example 21 Oct 2005

- BNZ takes its Internet banking site down following a phishing scare
- Customers received emails directing them to what appeared to be a legitimate website
- Asks customer to enter bank account information, including PIN numbers, which are then used to rob the account
- There has been a spate of similar scams in the past month
- BNZ is working with other banks, police and ISPs to investigate scammers

16

## Phishing Attack – Further Examples of Bank Sites Shutdown

- Kiwi Bank: 8 December 2005
- National Bank: 12 December 2005

17

## Social Engineering - Phishing

- Phishing attacks are getting more sophisticated, eg www.citibank.com in address bar of browser even though, because of hidden text, you are visiting a different web site [Refer to Web-based Application Attacks - URL Manipulation/Parameter Tampering]
- “Secure” versions are faked: e.g. https://www.hsbc.com/login

18

# 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: www.pwcrack.com
  - Can often find 10% of passwords
  - Demonstrates value of OTPs (One Time Passwords)

20

# 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

- Spyware is a similar term which includes:
  - keystroke, e-mail and chat loggers – records and sends information without user's knowledge
  - for password entry some sites use buttons rather than keys

21

# Spyware Example

- "Hacker takes 3 minutes to get your cash" - Sunday Times 6 March 2005
- Hacker installer spyware key logger in an Internet café
- Recent spyware comes from US firm Marketscore and "harvests" all transactions via an embedded spyware program
- Banks now prevent customers accessing via Internet banking if they have used Marketscore software. [14 March 2005]
- Adware is software installed to support advertising

22

# Viruses, Worms and Network Propagation Systems

- Viruses
  - 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
  - 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)
  - 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

## 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)*

28

# Keeping Up-to-Date with Attacks contd ..

- Microsoft security bulletins and update services:
  - Security Bulletins (eg MS05-019 August 2005)
    - www.microsoft.com/technet/security/bulletin
  - Microsoft Download Centre (security updates)
    - www.microsoft.com/downloads/results.aspx?displaylang=en&freetext=security_patch
  - Windows Update Web Site (consumer platform updates)
    - update.microsoft.com/windowsupdate/v6/default.aspx?ln=en-us
  - Microsoft Software Update Services (additional information)
    - www.microsoft.com/windowsserversystem/updateservices/evaluation/previous/default.mspx
  - Microsoft Baseline Security Analyser (MBSA)
    - www.microsoft.com/technet/security/tools/mbsahome.mspx

29

# Example – Microsoft Security Bulletin

- Microsoft Security Bulletin MS05-019
  - Vulnerabilities in TCP/IP
    - Issued: April 12, 2005
    - Updated: August 17, 2005
    - Version: 2.1
    - Security Rating: Critical
    - Impact of Vulnerabilities: Remote Code Execution

30

# Severity Ratings and Vulnerability Identifiers (August 2005)

| Vulnerability Identifiers | Impact of Vulnerability | Windows 98, 98 SE, ME | Windows 2000 | Windows XP Service Pack 1 | Windows XP Service Pack 2 | Windows Server 2003 |
|---|---|---|---|---|---|---|
| IP Validation Vulnerability – CAN-2005-0048 | Remote Code Execution | Not Critical | Critical | Critical | None | None |
| ICMP Connection Reset Vulnerability – CAN-2004-0790 | Denial of Service | Not Critical | Moderate | Moderate | Moderate | Moderate |
| ICMP Path MTU Vulnerability CAN-2004-1060 | Denial of Service | Not Critical | Moderate | Moderate | Moderate | Moderate |
| TCP Connection Reset Vulnerability – CAN-2004-0230 | Denial of Service | Not Critical | Low | Low | None | Low |
| Spoofed Connection Request Vulnerability – CAN-2005-0688 | Denial of Service | None | None | None | Low | Low |
| Aggregate Severity of All Vulnerabilities | | Not Critical | Critical | Critical | Moderate | Moderate |

31

# Severity Ratings and Vulnerability Identifiers (August 2005) contd …..

- IP Validation Vulnerability – CAN-2005-0048
  - Remote attackers can cause DOS and execute arbitrary code via crafted IP packets with malformed options
- ICMP Connection Reset Vulnerability – CAN-2004-0790
  - DOS (reset TCP connections) via spoofed ICMP error messages
- ICMP Path MTU Vulnerability - CAN-2004-1060
  - TCP/IP with Path Discovery permit DOS attacks in conjunction with forged ICMP options
- TCP Connection Reset Vulnerability – CAN-2004-0230
  - TCP with large windows makes it easier for attacker to determine sequence numbers and cause DOS attacks by (repeatedly) using TCP RST option
- Spoofed Connection Request Vulnerability – CAN-2005-0688
  - Unknown vulnerability in HTTP Anti Virus Proxy prevents viruses being detected in .cab and .zip files

32

## Severity Ratings and Vulnerability Identifiers (August 2005) contd …..

- An attacker who successfully exploited the most severe of these vulnerabilities could:
  - take complete control of an affected system
  - install programs - view, change, or delete data
  - create new accounts with full user rights
  - cause affected system to stop responding

33

## Some issues with patches…..

- Implementing new patches/updates can be easy in principle but difficult in practice …..
  - Most recent patches sometimes cause applications to fail / run incorrectly
  - Backtracking with patches can sometimes leave corrupted .dll files which subsequently can cause patches not to “stick” , eg SoBig
  - Patching large .dll files can be slow (even too late)
  - Work developing on updating *part* of .dll (few lines)
- MBSA (Microsoft’s Baseline Security Analyzer) – scans for missing security updates

34

## Computer Emergency Response Teams (certs)

- www.apcert.org (Asia-Pacific)
- www.auscert.org.au (Australia)
- www.gcsb.govt.nz/ccip (New Zealand)
- www.singcert.org.sg (Singapore)
- 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)

35

## Trojan Horse

- 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
- Rootkit – collection of tools (programs) that hacker uses to mask intrusion and obtain admin level access

# 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

## 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

## 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 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!!

# 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)

42

## 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

43

## The New Trend “Zero-day” Attacks

- Zero-day attacks take advantage of software vulnerability for which there are no available fixes
- Attacks take advantage of flaws before software makers can fix them
- May well be a significant issue in 2006
- Emphasises importance of safe configuration policies and good incident reporting systems
- For example ……

44

## The New Trend “Zero-day” Attacks

- Malicious hackers are getting faster at exploiting flaws. The 2003 Blaster worm - one of the most virulent ever - hit the Internet barely a month after Microsoft released a patch for the flaw it exploited
- A variant - Nachi, carrying a dangerous payload, hit users less than a week later
- In contrast, Jan 2003 Slammer took eight months to appear after vulnerability it targeted was disclosed
- Timelines are collapsing. It is only a matter of time before users see attacks against flaws not yet disclosed or for which no patches are available

45

## Buffer Overflow - Common Attack Method

- Technique used to gain remote execution on host
- Takes advantage of inadequate buffer boundary checking in applications/services
- Often involves overwriting return addresses on the stack
- Involves sending executable code as binary data within an attack data stream, usually carefully crafted to be located at specific position within a buffer
- May be complicated by the need to encode the packet, eg Base64, uuencode

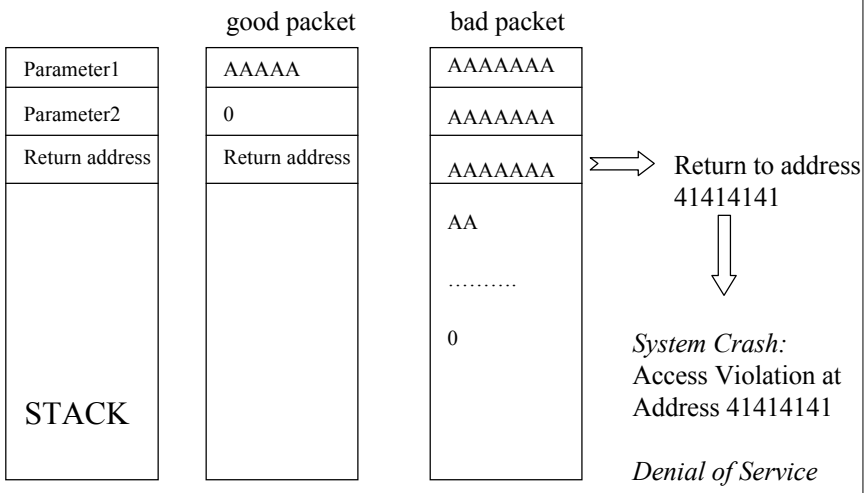
46

# 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 – (see note)

47

# Buffer Overflow - contd



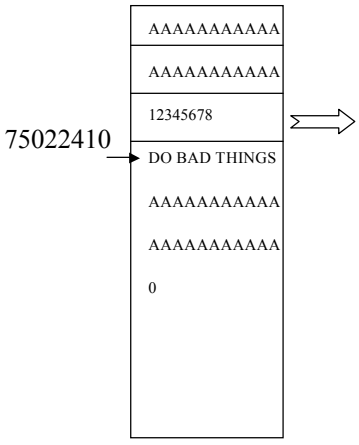

48

# 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)

49

# Buffer Overflow - contd




Return to address
12345678

| | |
|---|---|
| EAX | 0 |
| EBX | 12345660 |
| ECX | 75022410 |

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

***Voila!***

50

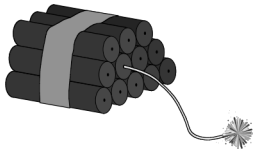
## Buffer Overflow - contd

- 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)

51

## Network Layer Attacks

- IP Spoofing (Masquerading)
- TCP Session Hijacking
- TCP Sequence Number Attack
- Web-based Application Attacks



# Threats to TCP/IP

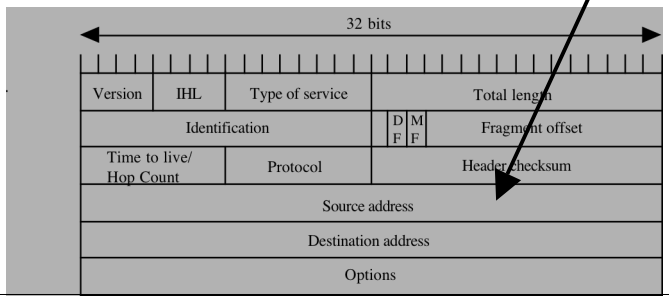
- IP Spoofing
- TCP Sequence Number Attack
- TCP Session Hijacking

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




54

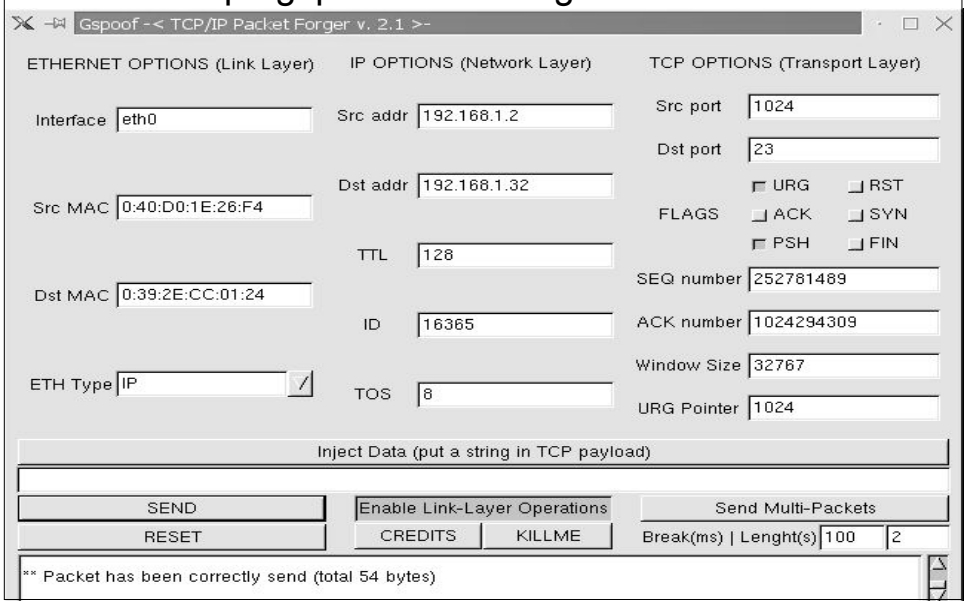
# IP Spoofing

- 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
- Spoofing can be used to hijack a domain by returning a fake DNS reply to the enquiry
- IP spoofing combines with TCP sequence number attack …

55

# Spoofing an IP Packet

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



# Threats to TCP/IP

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

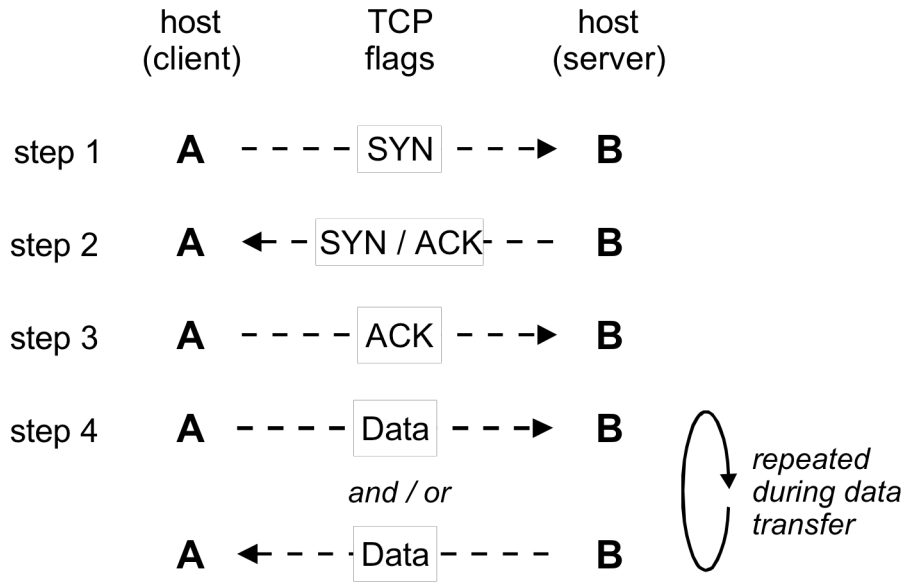
Often combined

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

# TCP Sequence Number Attack

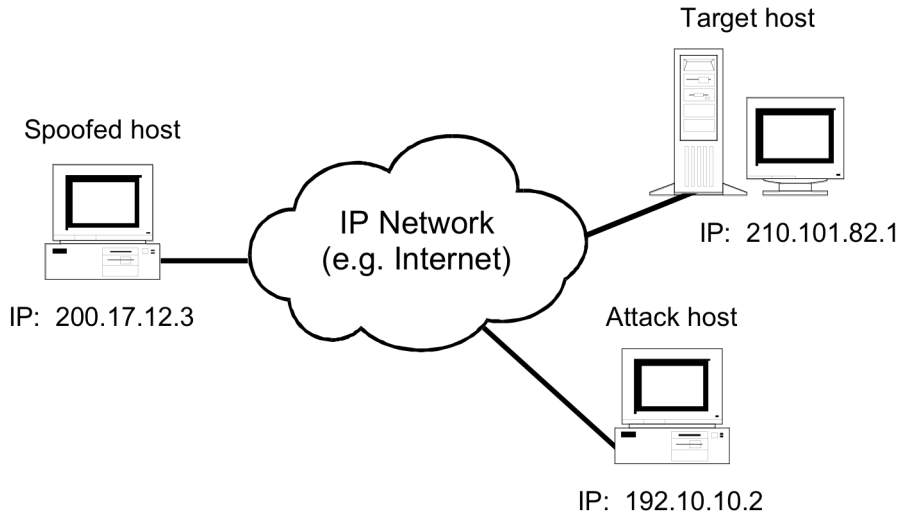
- TCP sequence number prediction takes advantage of TCP's sequenced data delivery
- If attacker determines correct sequence number then they can generate own TCP segments
- Two methods:
  - attack TCP handshake (TCP (IP) spoofing)
  - take over legitimate session (TCP hijacking)

58



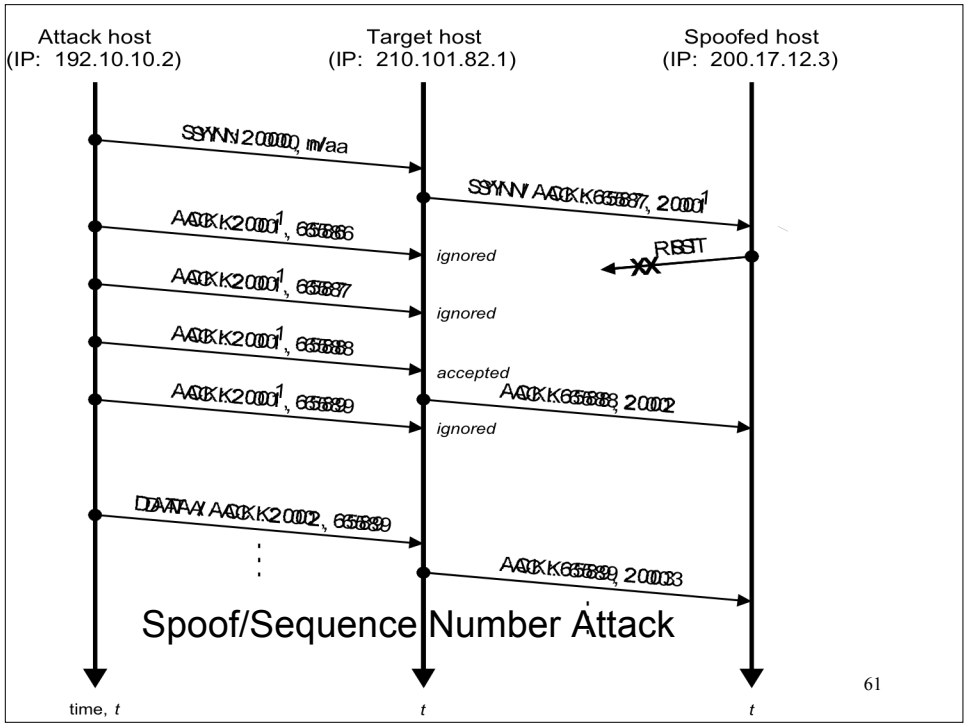

Can Attack TCP Handshake or Data Transfer

59




Spoof/Sequence Number Attack

60

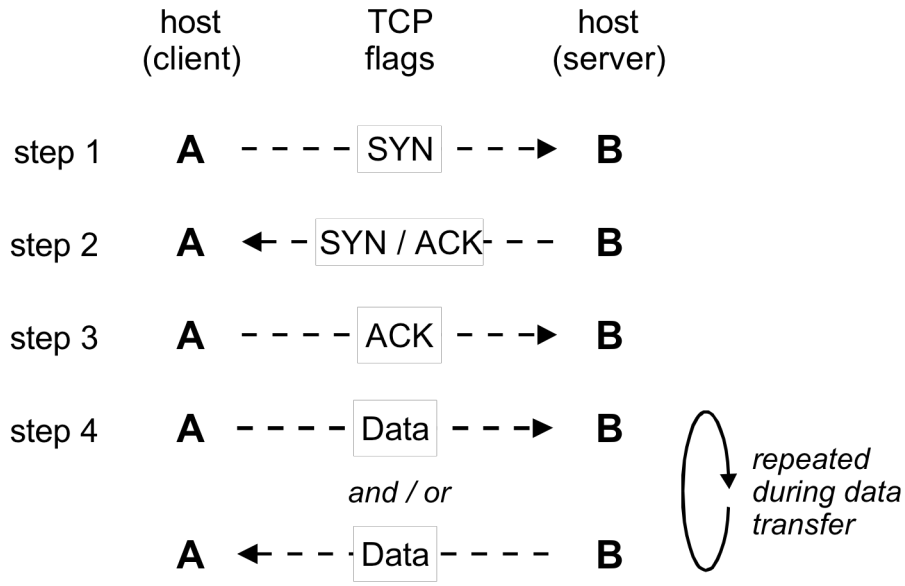



# Threats to TCP/IP

- 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*



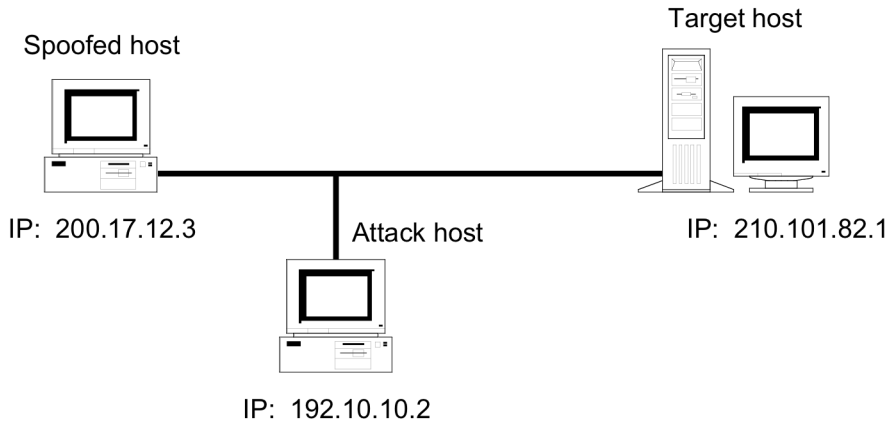

Can Attack TCP Handshake or Data Transfer

63

# TCP Session Hijacking

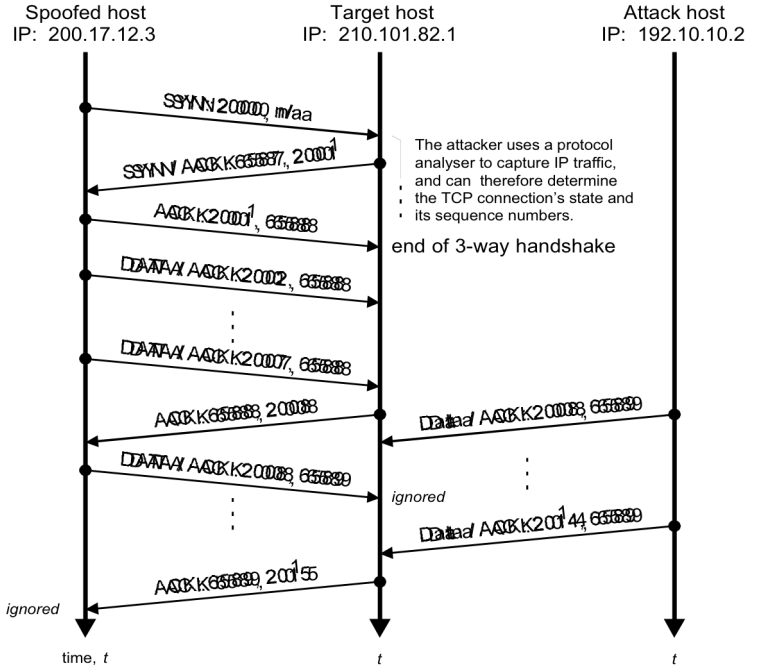
- TCP session hijacking used in conjunction with IP spoofing and TCP sequence number attack
- Can be used to take over TCP applications like Telnet, FTP, rlogin
- Once attacker has TCP segment sequence they can take over connection
- All packets then sent by hijacked (spoofed) host will be ignored by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

64




TCP Session Hijacking

65




TCP Session Hijacking

66

# 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 expected range (spoofed addresses)
- Trusted hosts (eg .rhosts) should only be used with authentication and encryption
- Correctly configure firewall

67

# Web-based Application Attacks

- Input Validation and Uploading Files
- Cross Site Scripting
- Cookie Poisoning
- Execution Through Scripts and Applets
- URL Manipulation/Parameter Tampering
- Hidden Field Manipulation
- Header Field / Client Manipulation
- Database Attacks / SQL Injection
- Others: Backup file extensions, default files and directories, error messages, script commands ……

68

# Web-based Application Attacks - Input Validation and Uploading

- Data received from clients without appropriate validation is risky, possibly resulting in:
  - command execution
  - authentication bypass
  - information disclosure
  - account hijacking
  - denial of service, etc
- Client side validation could be removed from HTML pages

69

# Web-based Application Attacks - Input Validation and Uploading

- Filename / type must be validated to avoid uploading malicious files which could be used to gain access to server
- Directory permissions must be set accordingly on folders where files are uploaded
- Uploaded files must have file name, type and extension checked by validation routines

70

# Web-based Application Attacks - Cross Site Scripting

- Involves embedding script within web application which can result in:
  - faked web pages
  - cookie theft
  - unauthourised application usage
  - password and data theft
- Usually occurs on pages that allow for input, eg guest book or web form [see text]
- In July 2004, 3 of Australia's 4 largest banks were shown to be vulnerable to cross site scripting attacks



# Web-based Application Attacks - Cookie Poisoning

- Cookie poisoning involves modifying a cookie so that web application is deceived into giving away sensitive data
- Data is stored on client side so no cookie data should be trusted
- Cookies should be encrypted and hash stored so application can detect cookie tampering
- Cookie timeouts are a security issue as other users can use back button or browser cache to access restricted areas [see firewall configuration - remove cookies]

# Web-based Application Attacks - Execution Through Scripts and Applets

- If unvalidated user supplied data is used, may be possible for attacker to execute commands on server with higher levels of permission
- What commands can be run and consequences are dependent on OS and languages used
- Common system routines include:
  - system() shell() exec() open() passthru()
  - [see firewall configuration - Java/ActiveX applets]

73

# Web-based Application Attacks - URL Manipulation/Parameter Tampering

- URL should be validated and authenticated for current session
- Client has control of HTTP/HTTPS and associated parameters
- POST (submitting web pages) prevents parameters from being stored in browser's cache but does not prevent attacker from manipulating data
  - [see firewall configuration - deny submissions]

74

# Web-based Application Attacks - URL Manipulation/Parameter Tampering

- URL-encoded input can be used to disguise malicious code for use in attacks
- Valid usage:
  - http://<server>/showcode.asp?source=example.asp
- Invalid usage caught by simple checking for .../.../
  - http://<server>/showcode.asp?source=../../../../winnt/repair/ray
- Invalid usage bypassed by simple checking
  - http://<server>/showcode.asp?source=%2e%2e%2f%2e%2e%2fwinnt/repair/ray
  - [see firewall configuration - deny submissions]

75

# Web-based Application Attacks - Hidden Field Manipulation

- Web pages can use hidden fields, which can contain values to be submitted to application but not displayed
- Saving a page locally, editing values and then loading and submitting new page an attacker can modify these hidden values
- Could result in authentication bypass, price changing, command execution or account hijacking

76

# Web-based Application Attacks - Header Field / Client Manipulation

- Web browser uses HTTP headers to pass information to/from web applications
- Header fields sent from client should be validated before being used by application
- Attacks possible by header field manipulation:
  - SQL injection
  - command execution
  - cross site scripting
  - [see firewall configuration - remove client connection / unknown headers]

77

# Web-based Application Attacks - Database Attacks / SQL Injection

- Attacker can alter existing SQL calls, bypass security measures, gain access to unauthourised data or execute commands on database server
- Passing unvalidated data to database can result in buffer overflow and related attacks
- Attacker does not need to know username/password to exploit

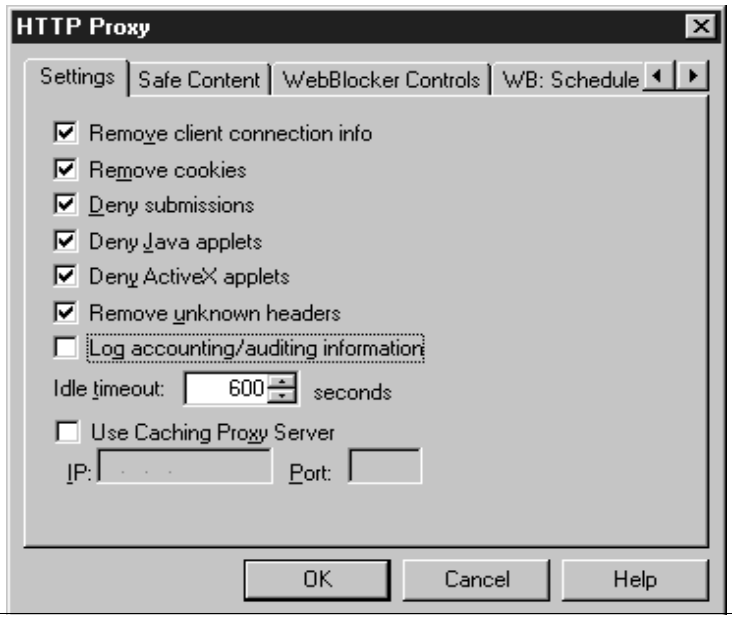
78

# Web-based Application Attacks - Database Attacks / SQL Injection

- SQL Injection examples:
  - ; - semicolon for end of command and multiple queries
  - %0a%0d - new line carriage return for multiple queries
  - ‘ and” - quotes, termination of strings
  - -- /**/ - comments in Microsoft’s SQL
  - EXEC - execute a stored procedure
- Robust web application protection needed

79

# Controlling Web Attacks at Firewall




80

# Web-based Application Attacks - Protection ….

- Many of these attacks can result if web application is:
  - poorly designed
  - poorly configured
  - poorly patched
- Many firewalls provide some filtering via http stateful packet inspection. A combination of well configured web server + sophisticated input validation + well configured firewall application proxies are essential
- Many web applications need to run over SSL/TLS



# 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

# Denial of Service Attacks

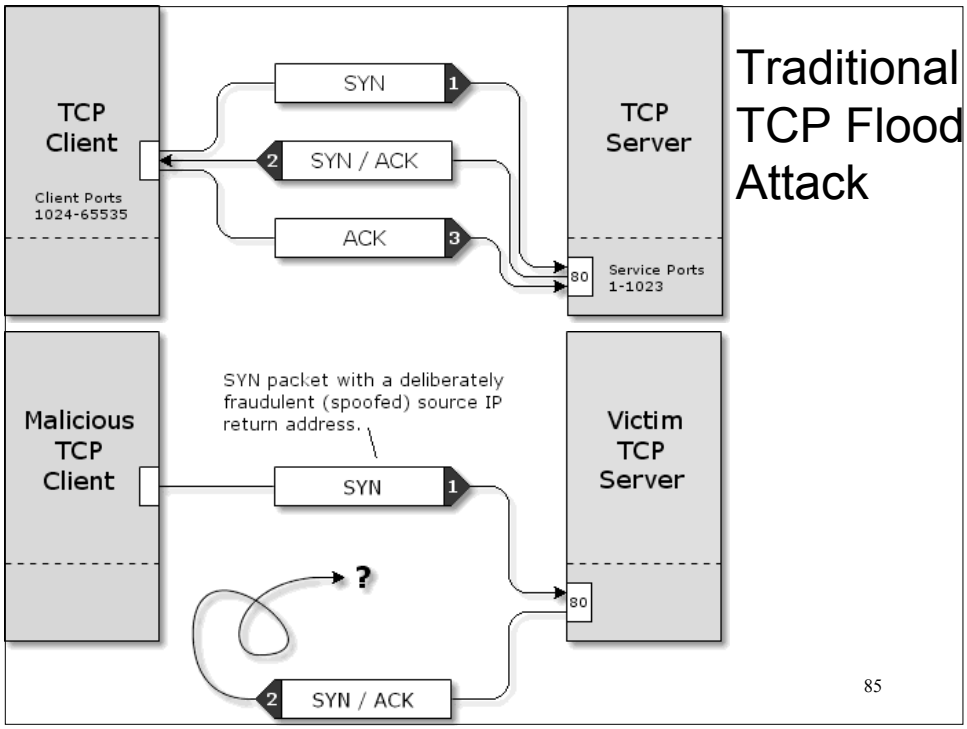
- DOS attacks broadly classified:
  - Bandwidth/throughput Attacks
    - Flooding to exhaust network resources
  - Protocol Attacks
    - TCP SYN flood, Smurf, etc
  - Software Exploits
    - Exploiting weaknesses in OS

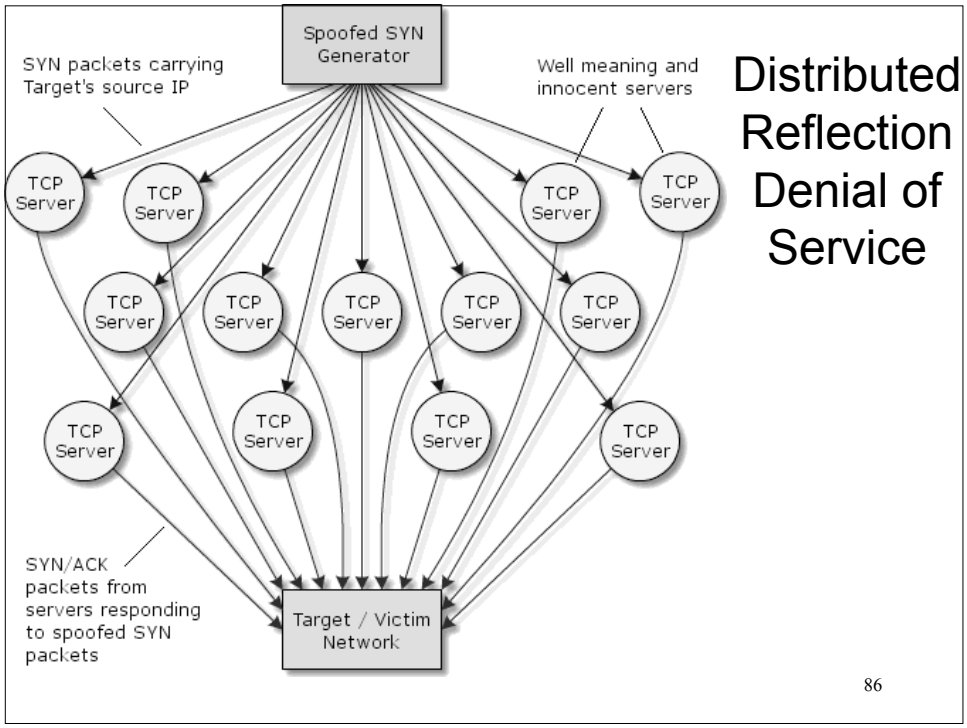
83

# (Distributed) Denial of Service Attacks

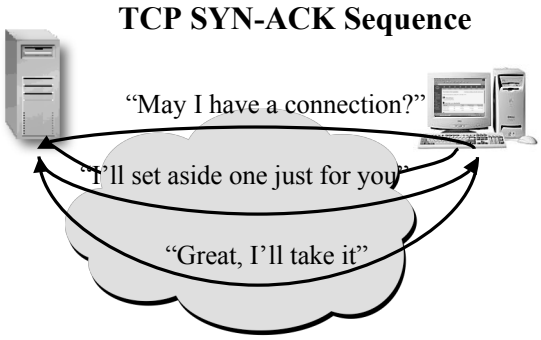
- Distributed DOS attack requires co-ordination from multiple sites
- Two categories:
  - Operating System Attacks - exploit known weakness and vulnerabilities
  - Network Attacks - exploit limitations of network resources, eg flooding
- www.packetstormsecurity.org has plenty of attack tools available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

84

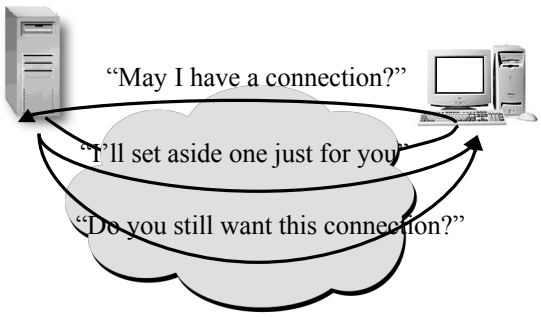

Traditional TCP Flood Attack
TCP Client
Client Ports 1024-65535
SYN
1
2
SYN / ACK
ACK
3
TCP Server
80
Service Ports 1-1023
Malicious TCP Client
SYN packet with a deliberately fraudulent (spoofed) source IP return address.
SYN
1
?
Victim TCP Server
80
2
SYN / ACK
85


Distributed Reflection Denial of Service
Spoofed SYN Generator
SYN packets carrying Target's source IP
Well meaning and innocent servers
TCP Server
SYN/ACK packets from servers responding to spoofed SYN packets
Target / Victim Network
86

# Normal TCP Connection Set-up



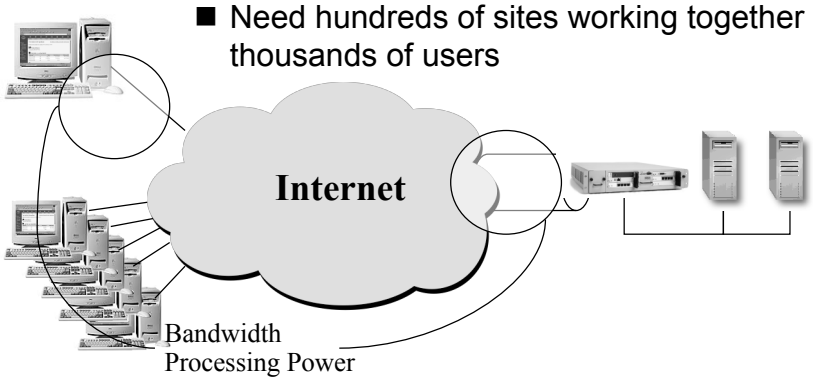

# Abnormal TCP Connection Set-up



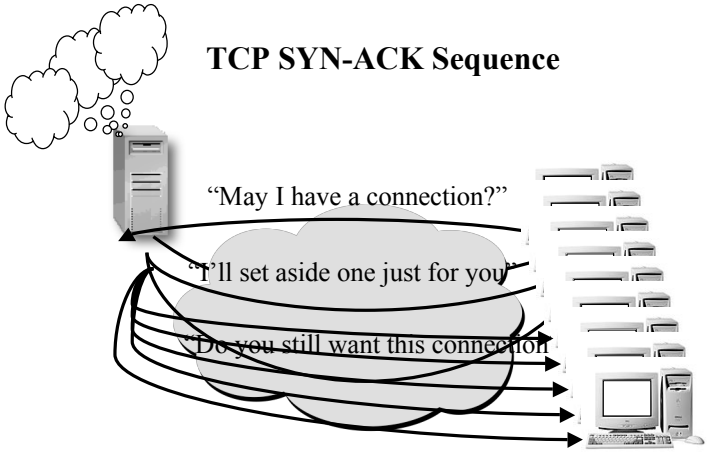

- Connection Setup Incomplete

# 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



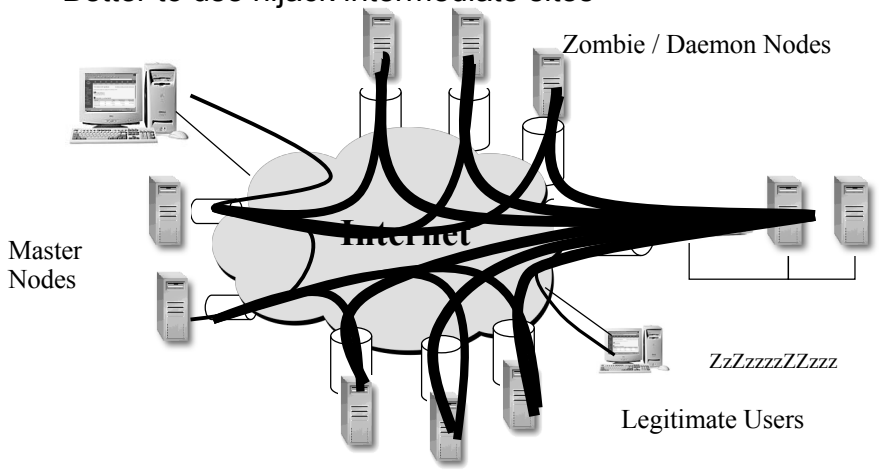

# Organised DOS Attack




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

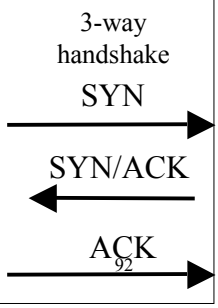
# Distributed DOS Attack

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




# 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

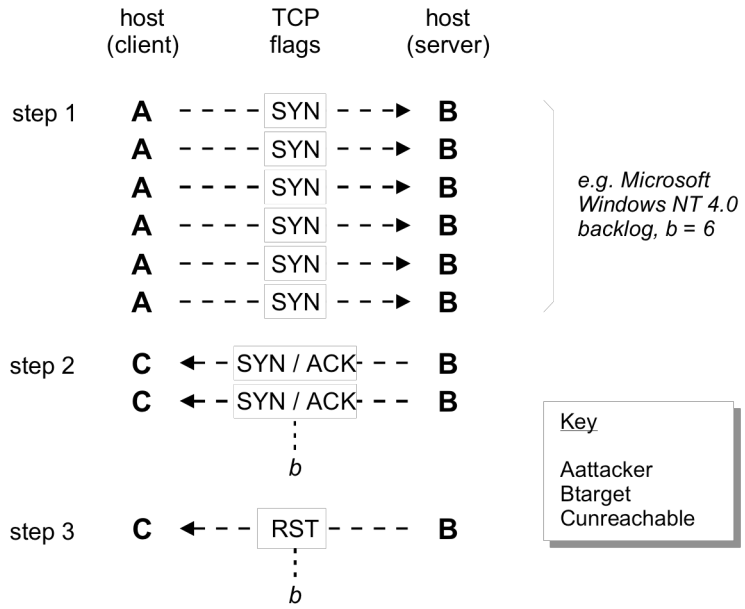



92

# SYN Flooding

- Number of half open connections limited
- Server rejects subsequent requests until existing requests time out → 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

93




TCP SYN Flood Attack

94

## Distributed Reflection Denial of Service

- Distributed Reflection Denial of Service (DRDoS) is like DDoS only attack's source is 'spoofed'
- In normal operation, a server receiving a SYN packet to establish a connection will respond with a SYN/ACK packet
- A malicious user may fake the source IP address of the original SYN packet, causing the server to send the SYN/ACK packet to a victim host
- Single malicious user can send same SYN packet to many servers - overwhelms victim with SYN/ACK packets
- DRDoS is preferable to simple DOS attacks due to the distribution of sources for the attack, and *simpler than DDOS* because infected hosts are not required; any host will perform as necessary
- DRDoS attack may occur on any port, making many traditional firewall defenses useless

95

## DOS – TCP Reflection Attacks

- Basic distributed reflection DOS attack, consists of an attacker (possibly using zombies) bouncing packets with forged source IP address off legitimate server so that server sends reply packets to forged source IP, i.e. victim
- This attack uses TCPs SYN/ACK mechanism, where reflection servers try to establish connection with victim by sending ACK packets
- This flood saturates victim. Once victim no longer respond with RST packets, things get worse as reflection servers start to retransmit ACK packets, assuming them to have been lost in transit.

96

## DOS – Shrew and Malicious Burst Attacks


- Low rate (Shrew) TCP Denial-of-Service attacks are new and exploit the RTO (minimum Retransmission TimeOut) property of TCP
- Basically a periodic short-burst attack which causes all TCP flows to back off and enter retransmission timeout state
- While TCP's congestion control algorithm is highly robust its implicit assumption of end-system cooperation results in vulnerability to short burst non-responsive flows
- Little is known about *low-rate* denial of service attacks
- Very difficult to identify

97

## 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

- 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)

# 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

103