Denial-of-Service Attacks

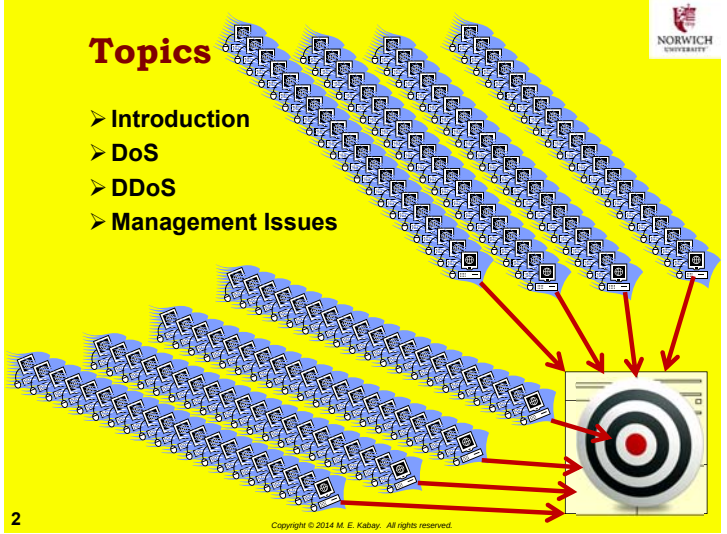
CSH6 Chapter 18

"Denial-of-Service Attacks"

Gary C. Kessler &
Diane E. Levine

Topics

- Introduction
- DoS
- DDoS
- Management Issues

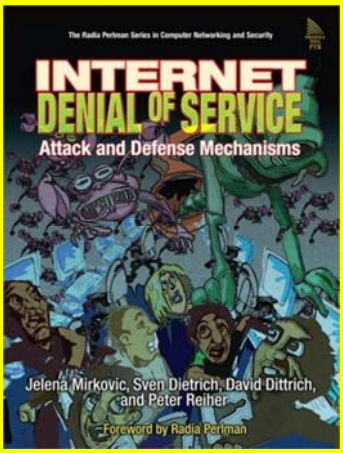


Introduction

- Fundamentals of DoS
  - "Denial of service" (no hyphens)
  - *"Denial-of-service"* attacks (adj)
  - *Intruder* attacks *victim*
  - Uses up scarce or non-renewable resources
    - ✓Bandwidth
    - ✓System elements (e.g., buffers, flags, counters)
  - Often attacker uses *daemons* for attacks
- Other types of DoS include user errors or physical attacks
  - Misconfiguration (e.g., bad parameters → catastrophe)
  - Malfunction (e.g., disk drive failure)
  - Destruction (e.g., physical damage such as e.g., *backhoe attack*)

DoS

- Overview
- History of DoS
- Costs of DoS
- Types of DoS
- Specific DoS Attacks
- Preventing & Responding to DoS

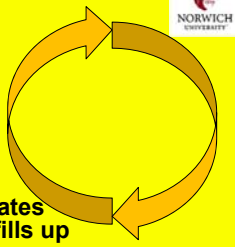


Overview (1)

- Denial-of-service attacks (DoS) & DDoS (Distributed DoS) attacks
  - Render target systems / networks unusable or inaccessible
  - Saturate resources or cause catastrophic errors
  - Difficult to prevent without widespread cooperation among ISPs
- DoS & DDoS attacks powerful tool for asymmetric warfare
  - Attacker resources can be modest
  - Consequences can be severe

Overview (2)

- Can also occur by mistakes causing positive feedback loops; e.g.,
- Autoforwarding between 2 e-mail accounts
  - When target fills up, sends bounce to original address which forwards bounce to full account which generates new bounce which… until mailbox fills up
- Out-of-office replies to lists
  - Message sent to everyone on list
  - Including absent person…
  - …whose e-mail sends out-of-office reply to entire list including same absent person….
- Competing Web-bots
  - E.g., automatically reducing price below each other's sale price….



History of DoS (1)

- Early systems subject to resource exhaustion
  - HP3000 console (early 1980s) received all system messages
    - ✓Logons, logoffs, requests for paper & tape
  - Pressing any key on console without pressing □ key blocked incoming system messages
  - System buffers filled up with messages
  - No further actions requiring notifications
    - ✓No one could finish logging on or off
    - ✓Anyone asking for tape/paper froze
- All systems that use obligatory user lockout at risk of DoS
  - Attacker need only log on to all userIDs with bogus password – locks everyone out

History of DoS (2)

- 1987-12: Christmas-Tree Worm
  - IBM internal networks
  - Grew explosively
  - Self-mailing graphic
  - Escaped into BITNET
  - Crashed systems
- 1988-11: Morris Worm
  - Probably launched by mistake
  - Demonstration program
  - Replicated through Internet
  - ~9,000 systems crashed or were deliberately taken off-line
  - Was about ½ to ¾ of Internet as it was then

History of DoS (3)

panix.com
Public Access Networks Corporation

Panix Attacks of September 1996

- Unknown criminal hacker attacked the PANIX Internet Service Provider
- "SYN-flooding attack"
  - Stream of fraudulent TCP/IP requests for connections
  - Non-existent Internet addresses
  - Overwhelmed server
  - Denied service to legitimate users
- TCP/IP specialists immediately developed patches to prevent recurrence

History of DoS (4)

- Forbes (Feb 1997)
  - Disgruntled employee George Parente deleted budgets, salary data
  - Crashed 5 of 8 network servers
  - Systems down 2 days – costs >$100K
  - Arrested by FBI – pled guilty
- Windows NT servers attacked (Mar 1998)
  - Repeated crashes
  - Included NASA, .mil, UCAL sites
- Australian mailstorm (May 1998)
  - Bureaucrat set autoreply + autoconfirmation to be sent to 2,000 users in network
  - Generated 150,000 messages in 4 hours
  - His own mailbox had 48,000 e-mails + 1,500/day arriving

History of DoS (5)

Melissa Virus (Mar 1999)

- CERT-CC reported fast-spreading new MS-Word macro virus
  - Melissa written by "Kwyjibo/VicodenES/ALT-F11" to infect Word documents
  - Uses victim's MAPI-standard e-mail address book
  - Sent copies of itself to 50 most e-mailed people
  - E-mail message w/ subject line "Important Message From <name>"

- Spread by David L. Smith (Aberdeen, NJ)
  - Spread faster than any previous virus
  - Took down ~100,000 e-mail servers
  - Estimated $80M damages
  - Convicted in 2002 of knowingly spreading computer virus
  - Sentenced to 20 months in federal prison + 100 hrs community service

Costs of DoS

- Direct costs often difficult to compute
- Indirect costs involve
  - Loss of immediate business
    - ✓Consumers switch to another Website if a vendor's system is too slow
  - Loss of customer confidence
    - ✓Many customers stay with latest supplier
  - Potential legal liability under SLAs (Service Level Agreements)
  - Costs of recovery
  - National security issues

Damages from DoS and DDoS: Tort

- Potential tort liability from allowing system to be used for harmful activities
  - Possible that victims of DoS and DDoS will sue *intermediate hosts* for contributory negligence
- Existing law in USA establishes requirements for best practices in preventing harm
  - Industry standards are common basis
  - Competitive pressures may move corporations to prevent misuse of their systems by DoS and DDoS tools

Specific DoS Attacks

- Destructive Devices (Malicious software)
  - Logic bombs
  - Viruses, worms, Trojans
  - Exploits of known vulnerabilities
- E-mail Bombing & E-mail Subscription-list Bombing
- Buffer Overflows
- Bandwidth Consumption
- Routing & DNS Attacks
- SYN Flooding
- Resource Starvation
- Java
- Router Attacks
- Other Resources

See *CSH6* Chapter 16, Malicious Code

E-mail-Bombing (1)

- In early days of e-mail (1980s), anyone could flood mailboxes
  - ISPs imposed strict limits on number of outbound e-mails
  - EULAs / Terms of Service explicitly forbid flooding
  - But could still use e-mail lists to flood victims
- 1996-08 — "Johnny [x]chaotic"
  - Subscribed dozens of people to hundreds of lists
  - Victims received up to 20,000 e-mail msg/day
  - Published rambling, incoherent manifesto
  - Became known as "UNAMAILER"
  - Struck again in December
- Caused serious re-evaluation of e-mail list management

E-mail Bombing (2)

- Root problem
  - Some list managers automatically subscribed people without verification
  - But now almost all lists verify authenticity of request
  - Send request for confirmation to supposed recipient
- But can still flood victim using automated subscription requests
  - Thus many list managers now use CAPTCHAs*

Completely Automated Public Turing test to tell Computers and Humans Apart

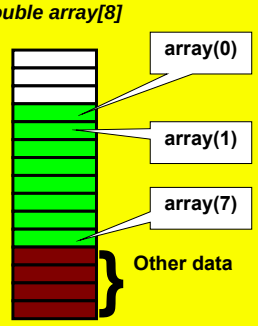
Buffer Overflows

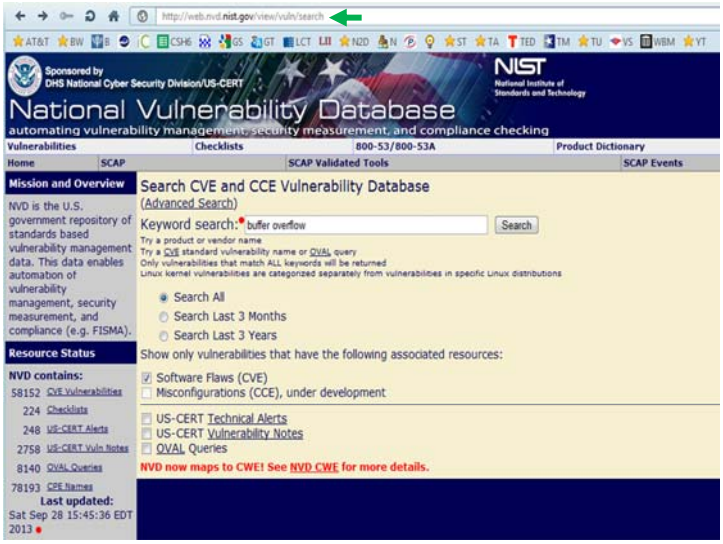
- What is a Buffer Overflow?
- Origin of Buffer Overflow Vulnerabilities
- Statistics on Overflows
- Consequences of Bounds Violations
- Bounds Violations in Interpreters
- Buffer Overflows Common Security Problem
- Example of Buffer Overflow Security Vulnerability
- Blaster as Example
- Fighting Buffer Overflows

What Is a Buffer Overflow?

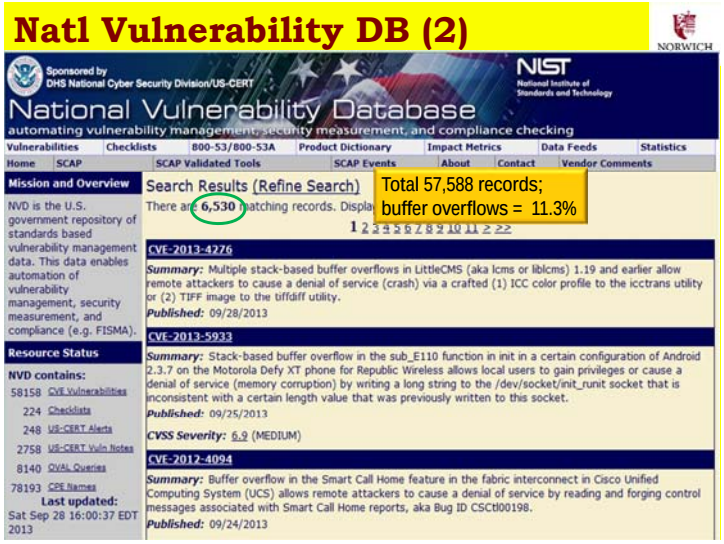
Programming concept:

- Define (declare, dimension)
  - list (array, indexed variable, string)
  - of certain size
- To reserve area of memory for specific use during execution



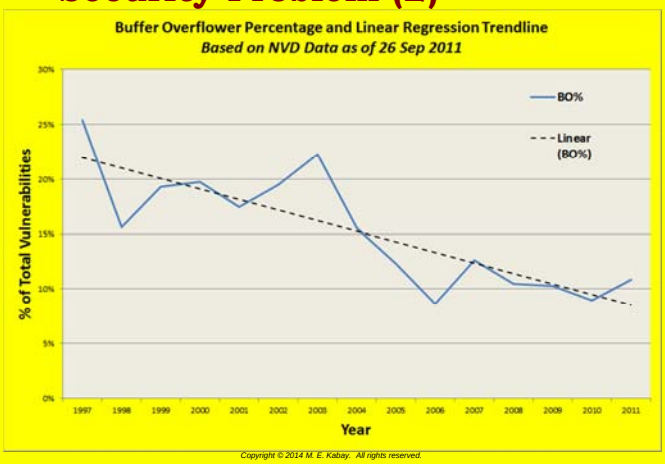


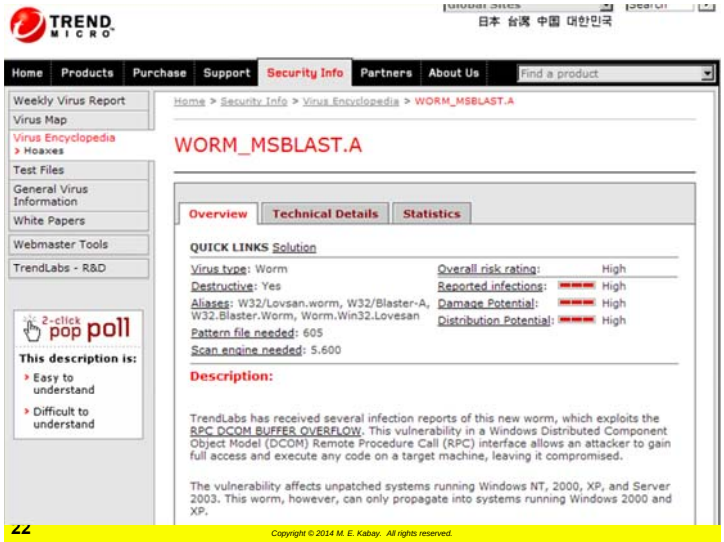
Natl Vulnerability DB (2)



Total 57,588 records; buffer overflows = 11.3%

Buffer Overflows Declining Security Problem (2)





This worm has been observed to continuously scan random IP addresses and send data to vulnerable systems on the network using port 135. On the following system dates, it performs a Distributed Denial Of Service attack against windowsupdate.com:

- On the 16th to the 31st day of the following months:
  - January
  - February
  - March
  - April
  - May
  - June
  - July
  - August
- Any day in the months of September to December.

Important: Users of affected systems are strongly advised to apply the necessary patches, which may be downloaded from the following Microsoft page:

Microsoft Security Bulletin MS03-026

Users are also advised to visit the following page for more information from Microsoft:

What You Should Know About the Blaster Worm and Its Variants

For general overview of the MSBLAST family of worms, please refer to the Virus Encyclopedia entry for WORM_MSBLAST.GEN.

Solution:

Important: To fully protect systems against this security threat, users are advised to apply the critical patches first before performing the Removal Instructions. The importance of applying these patches cannot be overstated and should be strictly implemented across the network. Cleaning the system without prior installation of the Microsoft patch may result to immediate reinfections or system instability.

Applying Patches

1. Apply the patches issued by Microsoft from the following page:

   Microsoft Security Bulletin MS03-026

2. TrendLabs also asks users to filter access to port 135 and allow trusted and internal sites only.

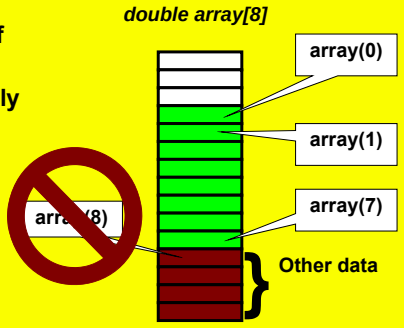
RPC DCOM Buffer Overflow Vulnerability Scanning Tool

TrendLabs advises users to download the scanning tool released by Microsoft that can identify host machines in their network that do not have the MS03-026 security patch installed.

This Microsoft Scanning Tool is available for download at: http://support.microsoft.com?kbid=826369.

Origin of Buffer Overflow Vulnerabilities

- In using a member of an array (an indexed variable), it is critically important to avoid addressing *out of bounds*
- Doing so is called a *bounds violation*
- Can corrupt data of other variables



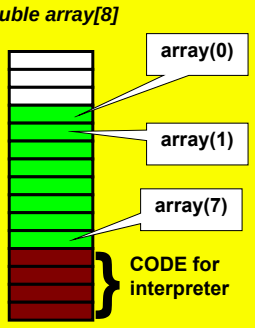
Consequences of Bounds Violations

Possible to see
- Compiler error
- Run-time error
- Program errors – bad results
- Program crash
- System crash

But most dangerous problem occurs in *interpreters*
- Programs that dynamically interpret instructions
- E.g., browsers, Web server programs

Bounds Violations in Interpreters

- Some interpreters read areas of data as instructions (code)
- Bounds violation can put *data* into *code* areas of working memory
- Thus *bad data* can become equivalent to *bad code*
- Can sometimes execute *arbitrary code*
- Obtain unauthorized privileges



Ping of Death

- IPv4 limits data block to 65,636 bytes
- *Ping of Death* attack uses this limit
- Break up data block into normal sized packets
- But these packets have sizes that add up to more than limit
- Get packets through gateway security because each packet seems acceptable
- But then packets are assembled into unacceptably large message
- Causes overflow in IP kernel
- System crashes

Fighting Buffer Overflows

- Programmers need to use good quality assurance techniques
  - ❑Test long input strings
  - ❑Test below, at and above boundary conditions
- System / network / security staff: *check* for new buffer overflows & install *patches*
  - ❑Use NVD frequently to find new vulnerabilities and remediation: http://nvd.nist.gov
  - ❑Subscribe to CERT-CC alerts from http://www.cert.org

Fighting Buffer Overflows (cont'd)

- Managers need to understand that *every buffer overflow is a failure of quality assurance*
- Stop allowing manufacturers to publish inadequately tested software as production versions
- Stop letting manufacturers push quality assurance onto the client base
- Complain loudly to manufacturers when there are buffer overflows in their software – and, if possible, buy competing products with better quality assurance

Bandwidth Consumption (1)

- Generating huge # packets directed to target
  - Local network; or
  - Generated remotely
- Key issue: does attacker have larger bandwidth available than victim?
  - If yes, can flood victim's input channels
  - Slow or block legitimate traffic
- Most common packet flooding uses ICMP
  - *Internet Control Message Protocol*
  - ICMP used for error & control messages
  - E.g., router notifies sender that destination node not available using ICMP*

*Example from *Computer Desktop Encyclopedia* http://computerlanguage.com/

Bandwidth Consumption (2)

- Bandwidth saturation (flooding)
  - SMURF
  - Fraggle
  - Kernel panic
    - ✓Land
    - ✓Teardrop

SMURF Attacks

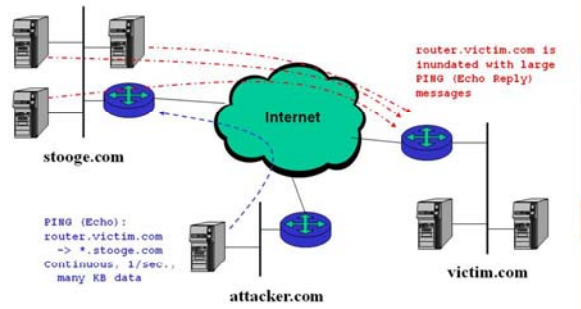


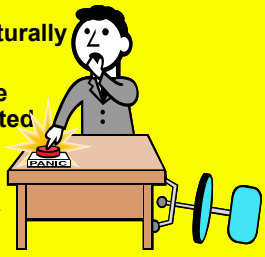
FIGURE 18.1. SMURF DoS attack.

Fraggle Attacks

- Analogous to SMURF attack but using UDP instead of ICMP
- Attacker sends spoofed UDP packets
  - User Datagram Protocol
  - Usually used for communicating over unreliable channels
  - Widely used for streaming audio, video, VoIP
- Bad UDP packets sent to broadcast address of amplifying network
  - Every responding node on system responds to victim address
  - Floods victim

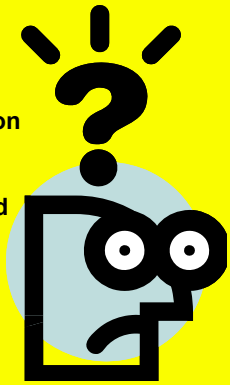
Kernel-Panic Attacks

- Impossible (illogical) condition causes code to fail
  - Different from bad coding
  - Condition should never naturally occur
  - Exploiting failure to include error handling for unexpected inputs
- Linux kernel v.2.2.0
  - Program normally used for printing shared-library info
  - If used to print core (memory-resident) files
  - Can overwrite areas of memory & cause reboot
- Ping of Death is classified as kernel panic attack



Land Attacks

- Bad TCP/IP packet parameters
  - SOURCE and DESTINATION ports set to same value
  - IP source address = destination address
- Causes 100% CPU utilization as impossible conditions are parsed by code
- Leads to system halt
- Successfully directed at "just about all operating systems" [CSH6 p 18.9]



Teardrop Attacks

- Result of receiving impossible packets
  - Normally, large packets broken into smaller pieces
  - Reassembled upon receipt
- But Teardrop IP packets overlap when reassembled
  - Cause system crash
  - Directed against Microsoft OSs & *nix

Resource Locking & Race Conditions

See *CSH6* Chapter 52 Application Controls

- Poor programming practices can lead to *deadlock* for local processes
  - Process A puts unconditional lock on Resource 1
  - Process B puts unconditional lock on Resource 2
  - Process A puts unconditional lock on Resource 2
  - Process B puts unconditional lock on Resource 1
- Bye bye! No way out except by *aborting* one process
- *Race condition* refers to dependency on specific timing
  - If Process B happens to lock R1 *after* Process A has unlocked R1 and R2, there is no hang
  - Thus the bad locking design causes an *intermittent* problem (tech support nightmare)

Routing & DNS Attacks

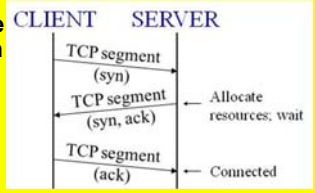
- Insert fraudulent data into Domain Name System
  - So domain name resolves to wrong IP address
- Eugene Kashpureff (1997)
  - Filed bad data with InterNIC causing recognition of fake TLDs .xxx, .mall, .nic, .per
  - Later inserted fake data to redirect browsers from networksolutions.com to his own Alternic site
  - Sentenced to 5 years probation

Eugene Kashpureff

- Gary Hoke (1999)
  - Redirected traffic to fake Bloomberg News Service page
  - Pump 'n' dump scheme to boost price of PairGain stock, then crash

SYN Flooding

- Exploits 3-way handshake for TCP hosts to establish connection
- SYN Flood sequence
  - Attacker initiates connection with fake origin on SYN packet
  - Server responds w/ usual SYN/ACK
  - Server waits for ACKnowledge response
  - But never comes – uses up finite resource for timeout (e.g., 10 seconds)
- Attacker launches barrage of these fake connection requests, saturating TCP stack
- Thus no one can connect



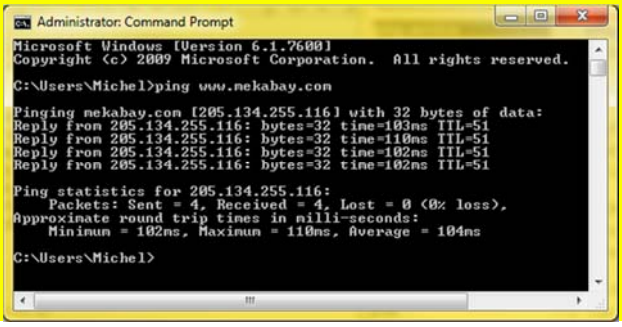
Resource Starvation

- Catch-all category for DoS attacks (or mistakes)
  - Any sequence that consumes resources & prevents authorized use qualifies
- Local inadvertent DoS by uninformed / careless users
  - In 1970s & 1980s, users would sometimes misconfigure their modems & eliminate timeout
    - ✓Thus modem could stay connected to phone line for days – block access to that line
  - Users can exceed their disk quotas and shut down processing if disk free space falls below critical levels
    - ✓In 1985, programmer at company where Prof Kabay was Dir Tech Services REMmed out PURGE command in JCL for temporary files
    - ✓Left so many TEMPnnnn files on disk that customer's account was frozen for exceeding disk quota

Ping Basics

Invented in 1983 by Mike Muuss http://ftp.arl.mil/~mike/
See http://ftp.arl.mil/~mike/ping.html

- ping xx.xx.xx.xx where xx are the IP address or the URL
  - Command-line command
  - "Are you there?" returns reply & lag time



Ping Flooding

- Send enormous number of normally-formatted *ping* packets to target
- Consume system resources trying to respond
- Slow down or stop responses to other requests

Java

- Java applets have been used for DoS
  - Exploits built on Java have caused browser internal errors to hang process
  - Others have caused endless loops of CPU and excessive use of RAM – hang browser
- Some attacks have rerouted DNS queries to fake DNS server
  - Phishing
  - Root compromise
- Java malformed code (e.g., Exploder) can cause reboot of Windows 9x system

See also "Mobile Code" in CSH6 Ch 17

Router Attacks

- Routers link organization to the Internet
- Attack on router blocks all 'Net access for all systems dependent on the router
  - National Vulnerability Database (NVD) reports 404 router vulnerabilities as of Sep 2013
  - http://nvd.nist.gov/
- Routers that have been exploited:
  - AlaxalA, Avici, AzTech, Century, Cisco, Hitachi, Linksys, Neostrada, Netgear, Proxim, Sweex, ZyXEL….

Other Resources

- See
  - Householder, A., A. Manion, L. Pesante, & G. M. Weaver (2001). "Managing the Threat of Denial-of-Service Attacks, v10.0" CERT/CC® http://www.cert.org/archive/pdf/Managing_DoS.pdf
  - Meadows, C. (2000). "A Framework for Denial of Service Analysis." Paper presented at the Information Survivability Workshop 2000 (Oct 24-26, 2000). http://www.cert.org/research/isw/isw2000/papers/37.pdf

Preventing & Responding to DoS (1)

- *Prevent* in preference to respond
- Harden operating system
  - Keep security in mind when choosing parameters for configuration
  - Monitor for vulnerabilities
  - Use latest revisions of software
  - Keep patches up to date
- Critical: packet filtering at network routers
  - Apply egress filtering & ingress filtering to block fraudulent origination and destination addresses (respectively)
- Block all broadcast messages & most ICMP traffic

Preventing & Responding to DoS (2)

- Reject Ping and traceroute
- Do not respond by flooding attacker address
  - Usually faked
  - May be attacking innocent victim
- If actual compromised system identifiable
  - Request intervention by service provider
  - Contact CERT/CC®
  - US victims may coordinate with law enforcement, including FBI
- More information after discussion of DDoS

DDoS

- Overview
- History of DDoS
- DDoS Terminology & Overview
- DDoS Tools
- Defenses Against DDoS

Overview of DDoS

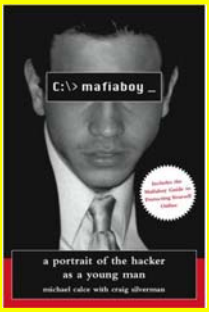
- Attacker subverts poorly secured system
- Controls tools to send large volumes of coordinated traffic against target
- Massive multiplier effect
- Packets arrive from many different sources
  - Makes packet filtering by source impossible
- Sources can be manipulated for PSYOP in information warfare – misleading impressions
- Techniques developed for DoS applied to DDoS

History of DDoS (1)

- Jun & Jul 1999: Trin00 (aka Trinoo)
  - Thought to be 1st DDoS tool
  - Tested on 2,000 systems worldwide
- Aug 1999: large-scale deployment of Trin00
  - >227 systems used as sources
  - Attacked 1 University of Minnesota computer – down 2 days
- Dec 1999: CERT/CC® issued CA-1999-17 discussing DDoS for 1st time
- Feb 2000: Mafiaboy attacks multiple e-commerce sites (see next slide)

History of DDoS (2)

- February 7, 2000 attack from "Mafiaboy"
  - Michael Calce, 15 year-old boy from Montréal area, Canada
  - Used a dial-up modem to control DDoS
- Effects
  - Yahoo.com inaccessible 3 hours
  - Est. $500,000 loss in revenue
  - Stock value fell 15%
- Feb 8:
  - Amazon.com 10 hours – $600,000 loss
  - Buy.com – 9.4% availability; stock lost 44% of value
  - CNN – user count fell to 5% of normal
  - eBay stock value fell 24%
- Feb 9:
  - E*Trade & ZDNet – completely unreachable
  - Charles Schwab – brokerage down – no exact figures



History of DDoS (3)

- May 2001: Attacks on Steve Gibson's GRC.com
  - Well-known security expert, writer, programmer
  - 13-year-old attacker used IRC bot
- Oct 2002: DNS servers attacked
  - All 13 top-level Domain Name System root servers swamped by DDoS for 2 hours
  - 9 servers went down – only 4 continued working
  - A few more hours might have knocked all the root servers off the 'Net – stopped Web

History of DDoS (4)

- DDoS as tool for extortion
  - Growing number of criminals (and criminal organizations) threaten DDoS attacks unless paid ransom
  - Demonstrate power by interrupting service
  - Most victims stay quiet about extortion
- Jan 2009: TechWatch digital TV site down
  - DDoS allegedly using 9,000 bots for SYN flood
  - 446Mbps avalanche of packets rose to 2 Gbps
  - Victim applied advanced traffic filters
  - Attackers demanded ransom

DDoS Attack on Social Networking Sites – Aug 2009

- Aug 6-8, 2009 – SNS under attack
  - Twitter down
  - LiveJournal down and up
  - Facebook slow
  - Gawker affected
  - Xbox Live
  - Some Google services
- Analysts believe attack was aimed at 1 blogger
  - *Cyxymu* outspoken critic of South Ossetia war
  - Writes in "Georgianised Russian"
  - DDoS attack blamed on Russian hackers*

*Example of hacktivism

DDoS Terminology & Overview

- *Terms* (synonyms)
  - *Intruder* (attacker, client)
  - *Master* (handler)
  - *Daemon* (agent, beast, bcast program, zombie)
  - *Victim* (target)
- Process
  - Intruder compromises insecure systems
  - Installs master program
  - Scans for thousands of weak systems
  - Installs daemon code to listen for instructions
  - Instructs *owned* systems to launch DDoS

Permission requested from Frans Charming for permanent use of image

DDoS Tools

- Trin00
- Tribe Flood Network
- Stacheldraht
- TFN2K
- Trinity
- Code Red Worm
- NIMDA
- Hidden Links in Web Pages or Programs

Trin00

- Appeared ~Jun/Jul 1999
- Distributed SYN flood
- TCP & UDP ports used
  - Masters listen on TCP port 27665 for instructions
  - Daemons listen on UDP port 27444 for masters
  - Masters listen on UDP port 31335 for daemons
- Intruder uses password (original: *betaalmostdone*)
- Programs
  - Master *master.c*
  - Daemon *ns.c*
- Operations
  - Specific commands and passwords for protocol
  - Characteristic traffic on specific ports – useful for detection

Tribe Flood Network (TFN)

- Appeared mid-1999
- Multi-attack DDoS system: ICMP flood, SYN flood, UDP flood, SMURF-like attacks
- Uses only ICMP traffic – difficult to detect
- Intruder supplies master with
  - IP address list of daemons
  - Type of attack
  - IP addresses of targets
  - Port number for SYN attack
- Programs
  - Tribe.c, td.c

Stacheldraht

- "Barbed wire" in German
- Appeared Aug 1999
- Similar to Trin00 & TFN
- Advances
  - Encrypted communication between Intruder & master
  - Automated daemon updates
- Programs
  - Intruder uses *telnetc/client.c*
  - Master is *mserv.c*
  - Daemons are *leaf/td.c*

TFN2K

- Tribe Flood Network 2K released Dec 1999
- Targets Unix & Windows NT servers
- More complex variant of TFN
  - Traffic harder to recognize & filter
  - Supports remote execution of commands
  - Hides source of attack using IP address spoofing
  - Transports traffic over many protocols
  - Sends decoy packets to conceal nodes
- Can also crash systems using malformed packets as in Teardrop & Land attacks

Trinity

- Sep 2000
- Also multi-tool
- Daemon installed on Linux machines using buffer overflow
- Communications with daemon via IRC or AOL ICQ instant messaging
  - Used chat room for communications

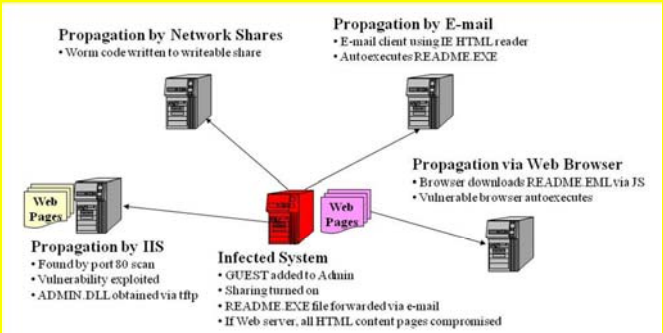
Carrie-Anne Moss as Trinity in *Matrix* films trilogy

Code Red Worm

- May 2001: buffer overflow discovered in Microsoft Internet Information Service (IIS) Indexing Service
  - Few IIS Servers were patched
  - Became DDoS daemons
- July 2001: Code Red Worm appeared
  - HTTP GET request to exploit buffer overflow
  - Spawns 99 daemon processes to attack "quasi-random" set of IP addresses
  - Displayed defaced Web page "…Hacked by Chinese!"
  - Days 20-27: flood phase – attacks old address of whitehouse.gov (IP 198.137.240.91)
  - On days 28-31 of each month, dormant
- Other variants followed (Code Red II, NIMDA)

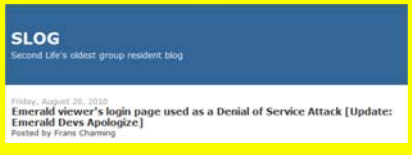
NIMDA

- Sep 2001 – "Admin" backwards
- Exploited multiple vulnerabilities in MS code



Hidden Links in Web Pages or Program

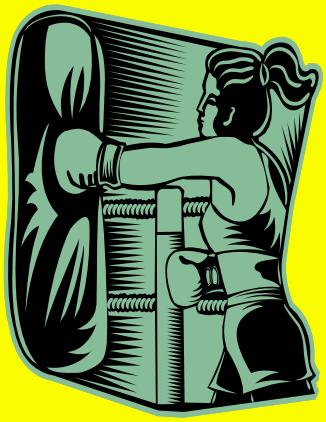
- Website *iheartanime.com*
  - Aug 2010: DDoS from all users of Emerald Viewer (EV)*
  - Open-source viewer for Second Life virtual world
- SLOG Second Life blog reported analysis
  - EV code modified to pull down 20 pages and 12 images from target servers
  - Massive interference in availability
- Developers "apologized" for their stupidity
  - Explained they were trying to lie about traffic to their site
  - Did not acknowledge illegality of attacks



http://secondslog.blogspot.com/2010/08/emerald-uses-loginpage-as-denial-of.html

Fighting DoS and DDoS

- Users
- System administrators
- Local Network Actions
- ISPs
- New Anti DoS Tools



Users

- Keep system up to date with updates, patches
- Use personal firewall and *think* before accepting *outbound* connection to Internet
- Verify that open ports are for known applications
- Don't accept executables from friends and colleagues – get valid version from trustworthy Web site yourself
- Don't download executables from untrustworthy sites
- Don't open any unexpected e-mail attachments
  - Be sure a human being sent it for specific, known reason
- Turn off "Hide file extension for known file types" in Windows options
- Use up-to-date browsers

System Administrators

- Maintain and examine log files
- Audit servers to ensure known-good status for all software
- Never install code from unknown or untrusted sources – and compile examined source if possible
- Subscribe to and follow best practices from
  - NIST CSRC http://csrc.nist.gov/publications/PubsSPs.html
  - CERT/CC http://www.cert.org
  - SANS http://www.sans.org
  - *Computer Security Handbook*! ☺
  - Bundesamt für Sicherheit in der Informationstechnik (BSI) http://www.bsi.de/english/gshb/index.htm

Local Network Actions

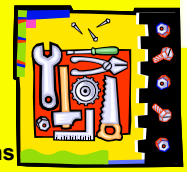
- Enable *egress filtering* to prevent any packet from passing if it uses forged IP headers
- Block all incoming packets addressed to a network broadcast address
- Turn off Directed Broadcast capability at router if feasible
- Discard any packet directed to RFC1918 private addresses
- Disable all unused application ports (esp. IRC or others known to be used by DDoS tools)
- Monitor network activity in real time to spot anomalies quickly

ISPs

- Ingress filtering – discard all packets from client if packet header shows wrong NET_ID
- Egress filtering – same rule to bar fraudulent packets
- Discard all inbound or outbound packets containing RFC1918 private addresses or other reserved addresses
- Disable IP directed broadcasts
- Monitor high-volume customers
- Join ISPSec Consortium – apply methods for cooperating to stop DoS and DDoS

http://www.icsalabs.com/html/communities/ispsec/index.shtml

New Anti-DoS Tools



- Network traffic monitors
  - Track normal patterns of traffic
  - Identify abnormal DDoS patterns
  - Shut down sources of fraudulent traffic
- RSA client puzzle
  - When connection flood detected, responds with cryptographic puzzle for client
  - Accept connections only given proper response
- IP Traceback
  - Mark some of the packets with path info
  - Or define ICMP Traceback message to victims
- Modify IP to stop address spoofing
  - Host Identity Payload
- Upgrade browsers to later versions

Commercial Products (1)

These are EXAMPLES, not ENDORSEMENTS

- ApplicCure dotDefender
  - Web application firewall
  - Session protection security engine
  - Blocks impersonation, high-volume traffic
  - http://tinyurl.com/m9q26s
- Arbor Networks
  - Peakflow DoS managed service
  - Gathers data from ISP networks
  - Establishes baseline to detect problems
  - Reconfigures routers to shut down flood
  - http://tinyurl.com/6g2z9f

Commercial Products (2)

- Lancope StealthWatch
  - Intrusion Detection System (IDS)
  - Includes DoS monitoring and response
    - ✓Detection
    - ✓Notification
    - ✓Traceback
    - ✓Forensics
  - http://www.lancope.com/
- Cisco Routers: "Configuring DoS Protection"
  - Detailed White Paper
  - http://tinyurl.com/5e8mvu

Management Issues

- Upper management discounts threat of DoS
  - Attacks must be targeted
  - "No one would attack us"
- But any site can become a host for daemons
  - Potential performance degradation
  - Damage to system integrity & reliability
  - Theoretical legal liability
- Failure to protect systems against exploitation increases power of DoS and DDoS attackers

Now go and study