Bugs, Flaws and Features

M. E. Kabay, PhD, CISSP

Associate Professor, Information Assurance Department of Computer Information Systems Norwich University, Northfield VT USA <u>mkabay@compuserve.com</u>

> NetworkWorld Dusseldorf, 2002-02



- •Bugs: Errors in programming
- •Flaws: Errors in program design
- •Features: Errors processed by the marketing department!







http://whatis.techtarget.com/definition/0,289893,sid9_gci214518,00.html

http://grc.com/optout.htm

http://www.logophilia.com/WordSpy/spyware.asp

http://www.acecmt.com/spyware.html

http://home.t-online.de/home/TschiTschi/spyware.htm

How does Spyware Enter a System?

- Install freeware, sharewareOften those that are ad-supported
- ➢ Some browser plugins □Offer new functions,

□New file format compatibility

Viruses & worms

□E-mail attachments

NetworkWorld Dusseldorf, 2002-02

http://www.lavasoftusa.com/faq.html

6

6



See http://www.suttondesigns.com/EnigmaBrowser/Spyware.html for a list of 406 spyware programs from A to Z



http://www.radiate.com/privacydisclosure.html

8



http://grc.com/oo/aureate.htm



http://accs-net.com/smallfish/conducent.htm



http://www.cometcursor.com/ http://accs-net.com/smallfish/comet.htm



http://users.rcn.com/rms2000/privacy/comet.htm



http://www.zdnet.com/zdnn/stories/news/0,4586,2774385,00.html



http://accs-net.com/smallfish/gohip.htm



http://www.web3000.com http://accs-net.com/smallfish/web3000.htm



http://www.spychecker.com/download.html



http://www.firewallguide.com/



18

NetworkWorld Dusseldorf, 2002-02







http://wuas.org/ http://www.thiefware.com/ http://stacks.msnbc.com/news/618966.asp



http://office.microsoft.com/assistance/2002/articles/oQuickSmartTags.aspx http://news.cnet.com/news/0-1003-200-6210768.html?tag=mn_hd http://www.alistapart.com/stories/smarttags/

E S	xamples of Scumware: urf+	
	Platitudes or Prophecy?	
	Sure, they sell. But are they <u>serious</u> ? <u>NEWSWEEK's</u> religion guru opines about the new spiritual best sellers.	
	By Kenneth L. Woodward	
	Aug. 27 issue Sociologists tell us that the United	
	States is experiencing a religious revival a third	
	"great awakening" echoing those of the 18th and	
	19th centuries. But if the best-seller lists are any guide, the revival looks more like a collective	
	leaving of the senses. The hottest books among	
	evangelical Christians, for example, is a religious	orkWorld
23		endorf, 2002-02

http://stacks.msnbc.com/news/618966.asp



Examples of Scumware: TopText

Dun & Bradstreet - http://www.dnb.com/

Provider of international and U.S. business credit information

Experian - http://www.experian.com

National consumer credit bureau and business credit reporting service

Equifax - http://www.equifax.com

One of three national <u>consumer credit</u> repositories

Trans Union - http://www.www.transunion.com

National repository of consumer credit information

<u>Credit Managers Association of California</u> http://www.cmaccom.com/

Business credit services

Business credit services

<u>CMA Business Credit Services</u> - http://www.creditservices.org/ Provides business credit reporting and commercial collections worldwide

25

Networkworio Dusseldorf, 2002-02



http://www.suniltanna.com/ezula.html http://stacks.msnbc.com/news/618966.asp





http://www.newsbytes.com/news/01/166676.html



http://www.farces.com/farces/992816200/ http://www.rbs2.com/moral.htm

29



http://www.whirlywiryweb.com/removeezula.htm http://www.whirlywiryweb.com/q/ezulasurf.asp http://www.whirlywiryweb.com/removesurfplus.htm http://www.petitiononline.com/toptext/







33



http://www.pestpatrol.com/Support/FAQ.asp#rate

What Kinds of Pests?

- ANSI Bomb: reprogram specific keys on keyboard
- Anarchy Documents
- Annoyance
- AOL Pest: password stealer, exploit, DoS attack, or ICQ hack
- Carding: Credit card fraud tools
- DDoS: Distributed Denial of Service (DDoS) zombie
- Disassembler

35

- > DoS: denial-of-service tool
- > Dropper: installs hostile code
- Exploit: break-in tools

- > Explosives documents
- Hostile Java
- > IRC War: Internet Relay Chat.
- > Key Logger: Keystroke Logger
- Loader: loads another program
- Lockpicking documents
- Mailbomber
- > NT Cracking document or tool
- > NT Security Scanner
- Netware Cracking document or tool
- Password Capture
- Password Cracker

NetworkWorld Dusseldorf, 2002-02



- Password Cracking Word List
- Phreaking Text
- Phreaking Tool
- Port Scanner
- Probe Tool
- RAT: Remote Administration Tool
- Ripper: tools for illegal copying of copyrighted works
- Sniffer: wiretap tools

- Spoofer: tools to forge IP address
- Spyware
- Theft documents
- Trojan
- > Trojan Creation Tool
- Virus Creation Tool
- > Virus Tutorial
- > War Dialer
- ≻ Worm

NetworkWorld Dusseldorf, 2002-02

36




See also http://www.pestpatrol.com/Whitepapers/Index.asp for a series of White Papers:

Sept 25, 2001 The Legal Risks of Computer Pests and Hacker Tools

June 21, 2001 A Comparison of Pest Detecting Tools

May 8, 2001 Denial of Service Attacks on the Rise

May 1, 2001 PestPatrol: Total Cost of Ownership. by Sal Salamone

Mar 29, 2001 Coping with RATs: A Look at the Problem of SubSeven and "Remote Administration Trojans"

Mar 26, 2001 Steps to Take To Check Your E-Commerce or Banking/Financial Site for NT-based Vulnerabilities

Jan 02, 2001 Detecting Pests: A Comparative Review

Jan 02, 2001 Beyond Viruses

Dec 28, 2000 About Spyware









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

43

NetworkWorld Dusseldorf, 2002-02



Bugs, Flaws und Features

ICAT	Your CVE Vulnerability S	Search Engine	X	0-00 / E	» N		
METABASE ST	SEARCH DOWNLOAD	NOTIFICATION	CONTACT	INFO TOP TEN L	.IST	Any Input valida	tion error
Welcome to ICAT: ICAT contains: Base updated: 1000 CAT is a searchable information on computer vulnerabilities translative search capability at a fine grapability at a fine support of updated by the Catalog search capability at a fine support of the following mapreciates the computer the CAT is a searchable the search searchable the searc	Search tips: All drop down means a time below to bol Search -> All Search -> All Search -> All Searc	Any	to create a quer by vendor or pro- by 6 Months HKh HKh HK H HK H H H	Soluct name	ICA ind col	AT is a sea dex of info mputer vu pability at	archable rmation on Inerabilities. earch
nie ICAT Metadase is a product of the <u>Computer Security</u> Division at the National Institute of Standards and Technology.	ICAT Deta ICAT Data Past Developers: Derek Dye,	retopets: <u>Peter Meil</u> , Eliz ibase Support: Susan Not. David Marks, Mark McLarr V Send Feedb	rapeth Boteler, Mid urbakhsh, Christina I non, Jorge Armenta /an Durme /aok to:ioat@nist.g	naer rKeiffy, Angelä Huh. Kingsberry, Rachel Glenr I, Jason Rosensweig, Joh	gra use pat	anularity a ers to vulr tch inform	nd links erability and ation.
cve.mitre.org	http://	icat.ni	st.go	v/icat.	cfn	<u>n</u>	NetworkWorld Dusseldorf, 2002-02

ICAT is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information.

See also information about the Common Vulnerabilities and Exposures (CVE) Database at http://cve.mitre.org $\,$



Buffer Overflows Common Security Problem (cont'd)

		Other	
	BO in that	Vulnerabilities	BO as % Total in
Year	year	in that year	Specific Year
1995	5	82	6%
1996	13	41	24%
1997	55	127	30%
1998	45	128	26%
1999	127	585	18%
2000	188	794	19%
2001	223	682	25%
			Network





http://icat.nist.gov/icat.cfm?cvename=CAN-2001-0728





- 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

51

NetworkWorld

Dusseldorf, 2002-02

51





For good links to overviews see

http://staff.washington.edu/dittrich/misc/ddos/

http://www.cert.org/advisories/CA-2000-01.html

http://www.denialinfo.com/

http://www.astanetworks.com/resources/

Fonseca, B. (2001). DDoS attacks are on the way. http://www.infoworld.com/articles/fe/xml/01/05/28/010528feedge.xml









57

Copyright © 2001 M. E. Kabay.

NetworkWorld Dusseldorf, 2002-02



Damages From DDoS	DoS and
February 7, 2000 attack	
□ Yahoo.com inaccessible 3	hours
ם \$500,000 loss in revenue	
≻ Feb 8:	
🗅 Amazon.com 10 hours \$	600,000 loss
□ Buy.com – 9.4% availabili	Σ γ
□ CNN – user count fell to 5	% of normal
□eBay	
≻ Feb 9:	
E*Trade – completely unre	eachable
□ ZDNet – also unreachable	
Charles Schwab – brokera	age down – no exact figures
	NetworkWorld Dusseldorf, 2002-02

Mazu Networks (2000). White Paper: The Denial of Serfice Problem. http://www.mazunetworks.com/wp_ddos.html

Radin, M. J. (2001). Distributed Denial of Service Attacks: Who Pays? http://www.mazunetworks.com/radin-toc.html

Costello, S. (2001). NIPC warns against increased DDoS attacks. http://www.nwfusion.com/news/2001/1105nipc.html



Moore, D., G. M. Voelker & S. Savage (2001). Inferring Internet Denial-of-Service Activity. USENIX Security 2001 Conference. Available as PDF download from http://www-cse.ucsd.edu/~savage/papers/UsenixSec01.pdf

Also available from http://www.astanetworks.com/resources/materials/nanog.pdf

Summary at http://www.caida.org/outreach/papers/backscatter/index.xml



Radin, M. J. (2001). Potential tort liability for damages due to DDoS attacks. Part II of "Distributed Denial of Service Attacks: Who Pays?" http://www.mazunetworks.com/radin-2.html



http://www.acm.org/ubiquity/views/m_kabay_1.html

Yasin, R. (2001). Techniques thwart DoS Attacks. http://www.internetwk.com/story/INW20010621S0003







SANS (2000). Help defeat denial of service attacks: Step-by-Step. http://www.sans.org/dosstep/index.htm

Fighting DoS: Network Administrators

- 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
- Join Alliance for Internet Security standards for preventing DoS tools from using your site <u>http://www.trusecure.co</u>m/html/partners/alliance.shtml Nature

ers/amarice.smin	NetworkWorld
	Dusseldorf, 2002-02

From Levine, D. E. & G. C. Kessler (2002). Denial of Service Attacks. Chapter 11 of Bosworth, S. & M. E. Kabay, eds (2002). *Computer Security Handbook, 4th Edition*. Wiley (New York); in press – publication date March 2002.

RFC 1918 defines a set of private IP addresses that are not to be routed on the Internet. These addresses include:

10.0.0/8	10.0.0-10.255.255.255	One Class A address
172.16.0.0/12	172.16.0.0-172.31.255.255	16 Class B addresses
192.168.0.0/16	192.168.0.0-192.168.255.255	256 Class C addresses

In addition, there are a number of reserved IP addresses that are never assigned to "public" networks, including:

0.0.0/32	Historical broadcast address
127.0.0.0/8	Loopback
169.254.0.0/16	Link-local Networks
192.0.2.0/24	TEST-NET
224.0.0.0/4	Class D Multicast address range
240.0.0/5	Class E Experimental address range
248.0.0.0/5	Unallocated
255.255.255.255/32	Broadcast

65







67

Copyright © 2001 M. E. Kabay.

NetworkWorld Dusseldorf, 2002-02



See

McCown, J. D. (2000). Applying filtering router technology to DDoS mitigation. http://www.trusecure.com/html/partners/guide_061201.shtml

Moskowitz, R. G. (2001). Host Identity Payload. http://homebase.htt-consult.com/~hip/

Fighting DoS:	Commercial
Products Now	Available

These are EXAMPLES, not ENDORSEMENTS

> Captus Networks: CaptIO

Policy-based intrusion detection + adaptive firewall technology

Traffic Limiting IDS uses network traffic profiling to set thresholds for stopping abuse

Mazu Networks – TrafficMaster

□Real-time gigabit/second packet filtering

□Spots and stops abusive traffic
 □Re-establishes normal filtering when DoS

stops

69

NetworkWorld Dusseldorf, 2002-02

Hardesty, L. (2001). Stemming the flood.

http://www.techreview.com/magazine/sep01/innovation5.asp

Hartje, R. (2001). Captus firewall/switch combo breaks new ground. http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2705626,00.html

http://www.captusnetworks.com/products.htm

http://www.mazunetworks.com/howitworks.html

http://biz.yahoo.com/prnews/011022/nem037_1.html

Andress, M. (2001). Get a positive ID on DDoS attackers. http://www.nwfusion.com/reviews/2001/0827rev.html

Messmer, E. (2001). Users put early anti-DDoS tools to test. http://www.nwfusion.com/archive/2001/126594_10-22-2001.html

Fighting DoS: Commercial Products (examples, cont'd)



Fonseca, B. (2001). N+I: Arbor Networks readies anti-DDoS package. http://www.infoworld.com/articles/hn/xml/01/05/08/010508hndos.xml

Arbor Networks

--in the news. http://www.arbornetworks.com/news?cid=5&tid=10

--product descriptions.

http://www.arbornetworks.com/standard?cid=4&tid=8

Messmer, E. (2001). Start-ups go on attack vs. denial-of-service threat. http://www.nwfusion.com/news/2001/0618antidos.html

Lancope Stealthwatch

--overview. http://www.lancope.com/products/index.htm

--DoS features. http://www.lancope.com/products/denial_service.htm





Microsoft (2001). What's new in security for Windows XP Professional and Windows XP Home Edition.

http://www.microsoft.com/windowsxp/pro/techinfo/planning/security/whatsnew/default.a sp

Andress, M. (2001). How will Windows XP cope with security? http://www.itworld.com/Comp/2218/IWD010514tcwindowsxp/

Farrow, R. (2001). Windows XP: Security by complexity. http://www.networkmagazine.com/article/NMG20011004S0009

Fontana, J. (2001). Microsoft boldly bundles again. http://www.nwfusion.com/news/2001/1008microsoft.html

Fontana, J. (2001). Tool assesses cost of Office XP upgrade. http://www.nwfusion.com/news/2001/0626asset.html

Williams, J. (2001). Windows XP Security: Internet Connection Firewall. http://netsecurity.about.com/library/weekly/aa071601a.htm


Farrow, R. (2001). Windows XP: Security by complexity. http://www.networkmagazine.com/article/NMG20011004S0009



Henderson, T. (2001). Windows XP: New desktop operating system gets high marks for reliability, a new interface and improved multimedia, but changes in the networking stack raise security issues. http://www.nwfusion.com/research/2001/1029feat3.html

Henderson, T. (2001). When an XP PC is politically correct. http://www.nwfusion.com/research/2001/1029feat3side.html

Tages, Flaws und Features States <t

Picture from http://grc.com/dos/zombiesoft.jpg Created by Karen Eliot http://antimedia.net/data/



Gibson, S. (2001). A brief summary of my position on the denial of service Windows XP raw socket controversy. http://grc.com/dos/xpsummary.htm

Gibson, S. (2001). Why Windows XP will be the denial-of-service exploitation tool of choice for Internet hackers everywhere. http://grc.com/dos/winxp.htm

Gibson, S. (2001). Windows XP Home Edition *Must* be Made More Secure. http://grc.com/dos/sockettome.htm



Gibson, S. (2001). Introducing SocketToMe and SocketLock. http://grc.com/dos/sockettome1.htm

Raw Socket Ab	use Prevention System
Socket Lock	Raw Socket Abuse Prevention System for Windows 2000 & XP. Freeware by Steve Gibson and Jeremy Collake.
Socket	Lock is Installed & Running
The SocketLocl are available to in the backgrou privilege, are pro and abuse-pron	 driver is installed and running. Full Raw Socket all Windows operating system processes operat nd. However, <u>ALL USERS</u>, regardless of their evented from accessing dangerous, unnecessary e raw sockets.



