Unauthorized Access & Denial of Service

CJ341 – Cyberlaw & Cybercrime
Lecture #3
M. E. Kabay, PhD, CISSP-ISSMP
D. J. Blythe, JD
School of Business & Management

Topics
- Sources of damage to computer systems
- Examples of system penetration
- Examples of Web vandalism
- Examples of denial of service

Rough Guesses About Sources of Damage to IT

Before 1993

Fire  Dishonest  Outsider

DEC  Water  Disgruntled  Virus

After 1993

Fire  Dishonest  Outsider

Disgruntled  Virus/ worms/ Trojans

See CSH5 Ch 10, “Understanding Studies and Surveys of Computer Crime.”
Also http://www.mekabay.com/methodology/crime_stats_methods.htm

Famous Cases of Penetration
- Mitnick
- DISA Report
- Citibank Hack
- More examples

1980-2003: Kevin Mitnick (1)
- Famous hacker born 1963
  - As young teenager, stole bus rides by using special punch for bus transfers
  - Phone phreaking, pranks, breakins using social engineering against DEC
- 1981: social engineering to enter PacBell
  - Juvenile court ordered psychological study
  - 1 year probation
- 1987: arrested for penetrating USC A
  - Stored stolen VAX VMS code on disks
- 1988: Arrested by FBI; sentenced 1989 to 1 year jail & 6 months rehabilitation

Kevin Mitnick (2)
- 1992: FBI tried to arrest him for stealing services from phone company computers
  - Went underground
- 1994: Insults Tsutomu Shimomura
  - Physicist & Internet security expert
  - Mitnick left rude messages on computer, voice-mail
  - Shimomura helped FBI track Mitnick
- 1995: FBI arrests Mitnick
- 1999: Convicted of wire fraud, computer fraud & illegal interception of wire communication
  - Sentenced to 46 months federal prison
Kevin Mitnick (3)

- Became cause célèbre among criminal hackers
  - FREE KEVIN defacements worldwide
  - Funniest: FREE KEVIN on Mexican Web site after release of KM
- 2000: released from prison
  - 3 years parole
  - Restricted access to computers
  - Profits from writing and speaking about criminal career used to reimburse victims
  - Founded own computer-security firm
  - Wrote books about defending against social engineering

Kevin Mitnick (4)

- Readings about the Mitnick case

DISA

- US DoD agency
- Real-time IT & communications support
- Core Mission Areas
  - Control & communications
  - Defense network management
  - Information assurance
- Web site home page
  - [http://www.disa.mil/](http://www.disa.mil/)

DISA Penetration Studies (1)

- The original DISA study lasted from 1994 through 1996
- 38,000 DoD unclassified computers
  - Tested by Red Teams / Tiger Teams
  - Easily-available penetration tools
  - 66% of the military Internet-visible systems & networks vulnerable to relatively trivial attack methods
  - Of 25,000 vulnerable systems, only 4% (~1,000) were run by system managers who noticed the intrusions
  - Of the systems where anyone noticed the problem, only about ½% (~5) actually reported the intrusions the way procedures dictated.

DISA Penetration Studies (2)

1997.03 — EDUPAGE

- InfoWar Division of Defense Information Systems Agency of US
- Retested 15,000 Pentagon computers
  - Warned system managers of vulnerabilities in previous audit
  - 90% of systems were still vulnerable
  - Recommended emphasizing response (immediate shutdown) instead of focusing solely on preventing penetrations

Penetration: Citibank Hack

1998.02 (events started 1994.07)

- Vladimir Levin of St Petersburg hacked Citibank computers
- Conspirator Alexei Lachmanov transferred US$2.8M to five Tel Aviv banks
- Admitted to attempting to withdraw US$940,000 from those accounts
- Three other members of the gang pleaded guilty
- Levin extradited 1997.09
Citibank Hack (2)
1998.02 -- Levin sentenced to 3 years, fined
- Vladimir Levin convicted by NYC court
- Transferred $12M in assets from Citibank
- Crime spotted after first $400K theft
- Citibank cooperated with FBI
- MORAL: report computer crime & help prosecute criminals

Robert Matthew Bentley
2008.06 – Pensacola, FL
- 21 year-old criminal hacker sentenced to 3 years in federal prison
- Pled guilty to charges of computer fraud
- Infected hundreds of computers in Europe
  - Adware installed illegally
  - Used computers in Florida to implant software on victims’ computers
- Paid by “Dollar Revenue” company in Europe
- Investigation and conviction required extensive international cooperation

Web Vandalism Classics
- CIA (1996.09)
- USAF (1996.12)
- NASA (1997.03)
- AirTran (1997.09)
- UNICEF (1998.01)
- US Dept Commerce (1998.02)
- SETI site (1999)
- Fort Monmouth (1999)
- Senate of the USA (twice)(1999)
- DEFCON 1999 (!)
Denial-of-Service (DoS) Attacks

- Flood resource – damage availability
- Can sometimes crash systems
- Techniques:
  - Mail-bombing (e.g., Johnny [x]Chaotic)
    - Subscribe victims to e-mail lists
  - SYN-flood
    - Launch fake attempts to connect
  - SMURF
    - Send ping to broadcast address using victim’s IP address as return
  - DDoS (e.g., Trinoo, TFN, Stacheldracht)
    - Use zombies to flood target with traffic

History of DoS

- 1987-12: Christmas-Tree Worm
  - IBM internal networks
  - Grew explosively
  - Self-mailing graphic
  - Escaped into BITNET
- 1988-11: Morris Worm
  - Probably launched by mistake
  - Demonstration program
  - Replicated through Internet
  - 9,000 systems crashed or were deliberately taken off-line

DoS: Mail-Bombing Via Lists 1996.08/12

- 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”
- 1996.12 — UNAMAILER struck again
  - Root problem
  - some list managers automatically subscribe people
  - should verifying authenticity of request
  - send request for confirmation
**DDoS – Distributed DoS**

- **1999-08: Trinoo**
  - Zombies on 227 computers
  - Flooded one computer at U. Minn
  - Down 2 days
- **Zombie:**
  - Slave program planted on vulnerable machines
  - Automatic search and infect process
  - 5 seconds per host
- **Master**
  - Sends out encrypted instruction on whom to attack at what time
  - Zombies listen on Internet connection
  - Act in concert

**Damages from DDoS**

- **February 2000:** “MafiaBoy” strikes Amazon, Buy.com, CNN, eBay, E*Trade, ZDNet.
- **Yahoo down 3 hours – lost $500,000**
- **Amazon down 10 hours – lost $600,000**
- Stock prices were depressed (see snapshots on next slides)

**MafiaBoy DDoS: eBay Stock**

24% Decline

**MafiaBoy DDoS: Yahoo**

15% Decline

**MafiaBoy DDoS: Buy.COM**

44% Decline

**DoS & DDoS: 2006**

- **January:** “Million Dollar Homepage” swamped by botnet with 100,000 computers
- **February:** CalState, U Michigan & UCLA computers subverted to create botnet
  - Generated $100K in false advertising revenue
  - Caused $150,000 damages to Seattle Northwest Hospital – and shut down ICU
- **March:**
  - Xerox WorkCenterPro copy machines can be shut down remotely
  - VeriSign reports massive attacks on DNS servers
DoS & DDoS: 2006 (cont’d)

- May: Millions of Blogs offline
  - Massive DDoS flood stopped access completely
  - Unavailable May 2-3
  - TypePad, LiveJournal, TypeKey, sixapart.com, movabletype.org and movabletype.com

DDoS: Killanet & Castlecops

- 2008.06 – Sacramento, CA
- Bot herder Gregory King, 21 pled guilty to charges of transmitting code to cause damage to protected computers
- Agreed to 2 years in federal prison
- Used botnets to generate DDoS against
  - Killanet: forum about graphic design, photography, gaming – attacked 2004-2006
- 2007.10.01 FBI arrested King – he threw laptop into garden before answering door
  - Contained digital evidence of his identity and crimes

DDoS in Georgian/Russian War 2008

- 2008.08 – Russia Disables Georgian Web Sites
- Massive demands on Georgian Web sites
  - Including Ministry of Foreign Affairs
  - Had to start posting press releases on GOOGLE site
- Also retaliatory DoS or DDoS against sites in South Ossetia and Russian news agency RIA Novosti
- Example of one aspect what is sometimes called information warfare or information conflict

Phlash Attacks: New DoS

- Rich Smith of HP Systems Security Labs
- Paper at EUSecWest Conference May 2008
- Demonstrated how to trash flash memory in high-tech networked devices; e.g.,
  - BIOS on computers
  - Driver store on printers
  - Disk drive controllers
  - Mobile phones
  - PDAs
- “Permanent Denial of Service” = PDoS by Phlash Attack
- Problem is that these devices have little or no security – including default passwords

Syrian Electronic Army (2013)

- Attacks on US newspapers from group claiming to be supporters of dictator of Syria, Bashar al-Assad
  - Financial Times
  - New York Times
  - Washington Post
- Attacked domain-name registrar
  - Websites unavailable on several days
- Also tried (but failed) to disrupt CNN site
- Spammed social networks (e.g., Facebook)

US Laws Defining Criminal Trespass with Computers

- Computer Fraud and Abuse Act
- Wire fraud
- ECPA

http://www.nytimes.com/2013/08/28/business/media/hacking-attack-is-suspected-on-times-web-site.html
or
http://tinyurl.com/pn6srcf
Computer Fraud and Abuse Act of 1986 (CFA, 18 USC § 1030)

- CFA is one of the most important US laws governing behavior in cyberspace
- Protects federal-interest computers
  - Governments at any level
  - Governmental agencies including military
  - Financial institutions
  - Medical institutions
  - Contractors to these institutions

CFA cont’d

- Prohibits unauthorized access
  - Obtaining or trafficking in confidential data
  - Installing unauthorized software
  - Mentions reckless disregard of consequences
  - Fines up to $250,000 & 5 years in prison
- Robert T. Morris convicted under CFA
  - Internet worm of 2 Nov 1988 → 9,000 computers down for 1-2 days
  - 400 hours community service
  - $10,500 fine
  - 3 years probation

Wire Fraud (18 USC § 1030(a)(5)(B)

- Fraudulent activity involving interstate wire (electronic) communications
- US vs Riggs 1990
  - Robert Riggs obtained enhanced-911 manual illegally from BellSouth
  - Craig Neidorf altered document, posted on BBS
  - Prosecuted under Wire Fraud Act
  - Case collapsed
    ✓ “secret” document worth “$100,000”
    ✓ available to public for $13 to anyone

Wire Fraud cont’d

- US vs LaMacchia (1994)
  - David LaMacchia was 21 year-old MIT student
  - Invited anyone to upload and download illegal copies of proprietary software
  - Could not be tried under copyright violations 17 USC § 506(a) because no personal monetary benefit
  - Indicted under Wire Fraud statute
  - Case dismissed
    ✓ No money, no fraud
    ✓ SCOTUS ruled that illegal copies of intellectual property are not property that is “stolen, converted or taken by fraud” under Stolen Property Act

ECPA – Electronic Communications Privacy *

- Bars intentional attack on wire, oral or electronic communications including
  - Interception
  - Attempt to intercept
  - Conspiracy to intercept
- Fines and imprisonment
  - Felony to use content of illegally-intercepted communications if perpetrator knows or should know it was illegally obtained
  - One party to a communication may authorize interception for lawful reason
* 18 USC § § 1367, 2232, 2510 et seq., 2701 et seq. 3117, 3121 et seq.

ECPA (2)

- Communications carriers
  - May intercept, disclose and use client communications
  - Must be as part of necessary procedures
  - Or for property or rights protection
  - Permission of sender or any recipient of a message can authorize disclosure or publication
- Wireless phone calls are also protected by ECPA
  - Cellular mobile phones
  - Wireless domestic phones
ECPA (3)

- ECPA does not apply to purely internal messaging
  - However, beware reasonable expectation of privacy
- Exceptions for law enforcement
  - With suitable warrant or subpoena
  - Under emergency conditions
- Case of Steve Jackson Games
  - Search and seizure of computers not warranted under ECPA

Now go and study