

Unauthorized Access & Denial of Service



CJ341 – Cyberlaw & Cybercrime Lecture #3

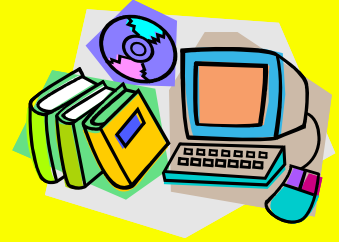
M. E. Kabay, PhD, CISSP-ISSMP
D. J. Blythe, JD
School of Business & Management

1

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Topics

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



2

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Rough Guesses About Sources of Damage to IT



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

3

Famous Cases of Penetration



- Mitnick
- DISA Report
- Citibank Hack
- More examples



4

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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 USCA
 - ❑ Stored stolen VAX VMS code on disks
- 1988: Arrested by FBI; sentenced 1989 to 1 year jail & 6 months rehabilitation



5

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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

6

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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



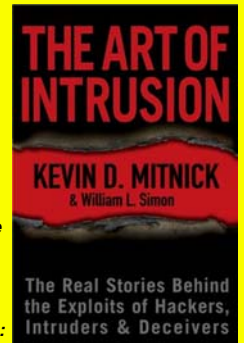
7

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Kevin Mitnick (4)



- Readings about the Mitnick case
 - ❑ Goodell, J. (1996). *The Cyberthief and the Samurai: The True Story of Kevin Mitnick—and the Man Who Hunted Him Down*. Dell (New York). ISBN 0-440-22205-2. xix + 328.
 - ❑ Hafner, K. & J. Markoff (1991). *Cyberpunk: Outlaws and Hackers on the Computer Frontier*. Touchstone Books, Simon & Schuster (New York). ISBN 0-671-77879-X. 368. Index.
 - ❑ Littman, J. (1996). *The Fugitive Game: Online with Kevin Mitnick—The Inside Story of the Great Cyberchase*. Little, Brown and Company (Boston). ISBN 0-316-5258-7. x + 383.
 - ❑ Shimomura, T. & J. Markoff (1996). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaw—by the Man Who Did It*. Hyperion (New York). ISBN 0-7868-6210-6. xii + 324. Index.



8

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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/>



9

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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 1/2% (~5) actually reported the intrusions the way procedures dictated.

10

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

DISA Penetration Studies (2)



- 1997.03 — EDUPAGE
- InfoWar Division of Defense Information Systems Agency of US
- Retested 15,000 Pentagon computers
 - ❑ Had 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

11

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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

12

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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 intensive 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)
- New York Times (1998.09)
- SETI site (1999)
- Fort Monmouth (1999)
- Senate of the USA (twice)(1999)
- DEFCON 1999 (!)



CIA

Welcome to the Central Stupidity Agency

We'd just like to say one thing. And that's

STOP LYING BO SKARINDER!!!

SLUTA LJUG BO SKARINDER!!!

Please choose one of the all the following categories below

Tower Through Resistance would like to say **FUCK YOU!** to the Central Intelligence Agency 'Podd' Web site... but we already know you're all lame assholes.

News that state of cyberspace is security chamber from skarpademantistry...

server has so few brains cells done so little for no one.

- [The Swedish Hackers Assesment Protocol #3 - SHA Protocol #3](#)
- [The Swedish Hackers Assesment Protocol #4 - CIA Protocol #4](#)
- [Flashback - The Flashback](#)
- [Subway - The Underground](#)

WELCOME TO THE TRUTH

USAF

You can learn all about gov't corruption here. Learn the secrets that they don't know want you to know. Well not really, I don't have time for that.

But trust me it's true. Take the time, and learn the truth yourself. After all information should always be free. Trust your mind not someone else's.

This is What your gov't is doing to you everyday

The thing is we all support the government whether we want to or not, as we pay taxes, etc. Why do we do this? Well the fact is we do this because we are told we have no choice, well the fact is we do have a choice, this gov't was founded on personal freedom.

Why should we give that up, for a congress of immoral greedy politicians? For a president that would be in jail other than for executive privilege. America was once a great nation, make it so again. Light back, and make this country great again.

NASA

Orbiter Thermal Protection System

(H4GIS > NASA)

Get341ngs from th3 m3mb3rs of H4GIS.

Our mission is to continue where our colleagues the ILF left off. During the next month, we the members of H4GIS, will be launching an attack on corporate America. All who profit from the misuse of the internet will fall victim to our upcoming reign of digital terrorism.

Our privileged and highly skilled members will stop at nothing until our presence is felt nationwide.

Even your most sophisticated firewalls are useless. We will demonstrate this in the upcoming weeks.

THE COMMERCIALIZATION OF THE INTERNET STOPS HERE

It's something else.

SO WE KILLED A FEW PEOPLE, BIG DEAL

AIRTRAN INTRODUCES NEW SERVICES, BEGINS STRATEGY TO KILL ALL AMERICANS!@#

ATLANTA, Sept. 24, 1997 - Vahjet Airlines today changed its name to AirTran Airlines and along with its merger partner AirTran Airways introduced a new business strategy designed to bring discernment to a broader travel audience. The airline said that its objective is to make air travel more attractive to business travelers and even more convenient for suicidal maniacs.

It seems Vahjet is attempting to pull an unethical "fast one" over on the public, while bailing out to a larger conglomerate. "Let's call ourselves AirTran then maybe someone will be dumb enough to get on board one of our flying death machines!#@#%!" says a gnggrots and fucks edit in the asshole with a 2 foot long salam.

"Over the past year we've narrowed our focus on the basis of our business with safety, reliability and operational excellence as our goal," led Coe, who joined the carrier in November 1996. He previously served as an associate in San Quentin and as passenger concierge 670564, he aged 42 soon. "AirTran's mission is to kill air travel customers who can actually afford to die. It's that simple. That's a significant change from our previous strategy, which was to offer the lowest-priced air transportation possible, without seatbelts or pilots," added Coe, who will be the chief executive of the merged airline and holding company.

**For an untimely death
800. AIRTRAN**

In the Atlanta area.
770.994.8258

In the Orlando area.
407.247.8726

MORE >

Copyright 1997 BoW Studios. All Rights Reserved.

19

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

unicef
United Nations Children's Fund

and DAMM bring you...

STARVIN' 4 KEVIN
(on hunger)
the too!

Oh here's the situ4tion. 4s we see it. n0 one is paying attention to the plight of the undergroun-d. fine, you had ur choice, n0w we make better. DAMM (Democr Against M4dd Mothers) and UNICEF have formed a coalition to put an end to the mistreatment of KEVIN MITNICK. Kevin has been held for over two years without trial n0r has he had adequate counsel. his imprisonment has been deemed unjust. 4ll 4s, Kevin is just a kid, and that's why UNICEF is all about, helping the children. speaking of children. On to the matter of our release Dm4.

If Kevin is n0t rel4sed by febr4ry 2nd (grounding's day), we begin the ultim4te h4tlocust.

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

20

SUId-USA/Inet

The actual site has been redesigned for easy access to 3,000 additional plank and hack-related philes, greater functionality, and a whole lot more! Cerefs to all members of SUId) and all friends.

Personal mag : i love u A--Y) from rew4
U May Want To Be Under Just Dependence
We Show u That U Take This Thing too simply ... from kilout
save amazony forest from somekool
Be wrong Be strong. from Adz
4 fuck d4dler looks, th4ts all guys

US Dept of Commerce

**Hack'd by Rewt4
for SUId**

A Service of the U.S. Department of What
Last Modified: February 03, 1998 | info@kilout.com | U.S. Department of Commerce

NORWICH UNIVERSITY

21

New York Times (1998. 09)

H4CK1NG FOR G1RL13Z

FIRST OFF, WE HAVE TO SAY.. WE OWN YER DUMB ASS. 4ND R3M3MB3R, DUMB ASS IS OPT3N CUTE 4SS. AND WE LIKE CUTE ASS.

3COND, TH3R3 AR3 80 MANY LOS3RS H3R3, ITZ HARD TO PICK WHICH TO INSULT THE MOST.

SINC3 WE AR3 NOW INTERN3T TERRORISTZ, W3 FIGURE WE SH0ULD DEMAND SOME RANSOM OR SOMETHING. SO, PAY US 104 GIRLIEZ, 6 BILLION IN N3WSP4P3R SUBSCRIPTIONZ, AND MAYBE A PRINTING PR3SS OR SOMETHING. NOT LIKS YOU GUYZ KNOW WHAT FAIR JOURNALISM IS ANYWAY. DUMB WHOR3Z.

NORWICH UNIVERSITY

22

SETI

WANTED:

NORWICH UNIVERSITY

23

Oh phuK n0.

n0t Our b0t@

n0t Our p3r0n4s smy b0t@# n0t@
y4k n0t w3 Owned y4.


th1s 1s 456c4t4 to all the f4gg0t from bump4s
to f4st n0/n0uth
may y4u r0t in h3ll, 44n3r3
w30 th1t. w3 c0uld gr4b p4p43. bu7 th3r3 w3 m4ght g0t /w0r0e0 on E Post, 4nd g0t Owned by th0se m34n f41 d000s.
4ll 1 h4v3 to say 4b0u7 th0se d000s, Is th4t It's all f4n3 g4m3 wh0m3v3r Owns wh0 fl47. and 1000z like y4u 1000g to 40n4
h333r3 4v3r3
b0t/n0t/n0t/n0t w3 Own y4u n0r.

NORWICH UNIVERSITY

24

Senate of the USA (1) (1999)

MOD KIX A\$\$



...the FBI may be all over the other groups, like those gH and IC groups, d00bagg g@t0r. MID make th0se ref0use 00K like a gr0up of sp0c@l@d00d@n@z@th@ FBI vs. MID in '99, BRING IT ON FUQKZ! (0TW NIPC 12 ALSO OWNED)

SOMETIMZ U GOTTA GO WITH A NAME U CAN TRUST. 4 SIMS, REGULATION 12 JUST A WAY 0F LIFE

Overed (0ne 34) th@ art of d0wnl0ading how stop@d a sp@c@n can b@, see velocity

BIG UP 2:

MOD/LOD/FR0K/FR0M/008/1/P&T
 BAH/9U/EL@/ZEL@40/ARSE/RSF
 TH@ 0R1@T@L S@H00L@919L@

5MAQ IN THE TETH 2:

ROM/8@91@/8@90/COB@/L@P
 TH@ VILK@O K0@3 W@9@1@R
 ALL TH@ F00K@ AT W@9@.MIL

25

Senate of the USA (2) (1999.06)



VARNA HACKING GROUP

LEGISLATIVE ACTIVITIES | LEARNING ABOUT THE SENATE | VISITING THE SENATE | CONTACTING THE SENATE | SEARCH

QUICK LIST

- Committee Hearing Schedule
- Yesterday's Senate Floor Activity
- Senate Art
- Senate History

YOU CAN STOP ONE, but you can NOT stop ALL!

Select a Press: [Go-Go Girls]

TRAVEL | **TRIP** | **TRIP** | **TRIP**

NEWS

Senator shot
 Senator Robert F. Kennedy (D-NY) was assassinated.

THE BATTLE

September 10, 1812
 By William Henry Powell
 1823-1879

NOTICE

Quick Links - Go directly to:

- Committee Membership List
- Senate Leadership Page
- Roll Call Vote Page
- Memberships Page

26



AdmCon DEFCON

ADM CON 7 is July 9-11th, 1999 on Planet Earth!

DEF CON 7.0 is owned! Here is some stuff that is planned

Can't make it to DEF CON? No problem. Delta Airlines is willing to sell you expensive business class tickets for twice their value. More information is available here.

Remote Owning facilities provided by the ADM Crew

Nerfing facilities provided by ANTONLINE. Use the anq-o-matic f0ss and get a live web cam shot of your mess@ges being br0@st!

This site soon mirrored in **ant0nline's** hacked web pages mirror!

Cult of the Dead Cow will announce NEW REMOTE ADMINISTRATION TOOL for kids!

ISS and NAJ associate to release all their 0-days for free!

27

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

28

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

29

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

30

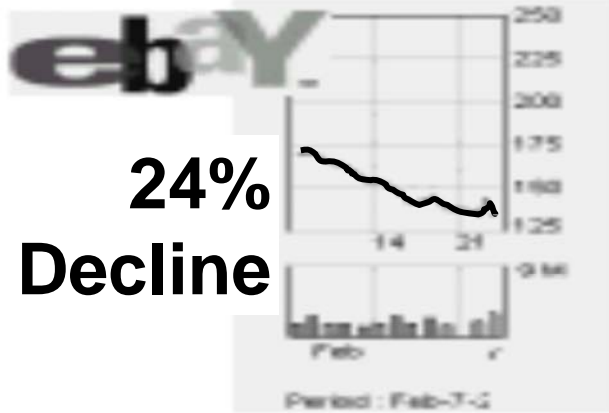
DDoS – Distributed DoS

- 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

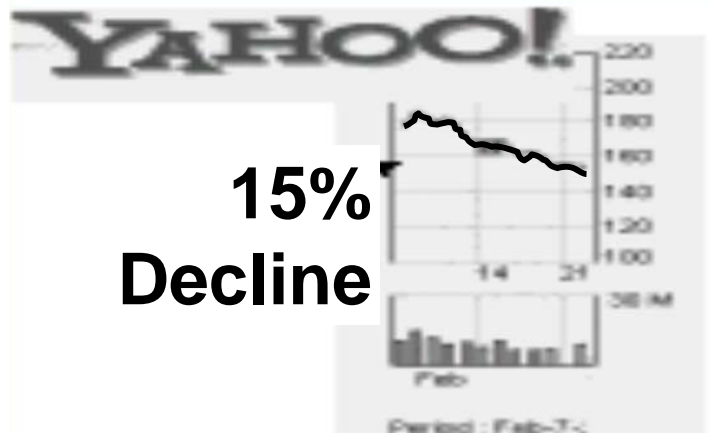
Damages from DDoS

- 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)

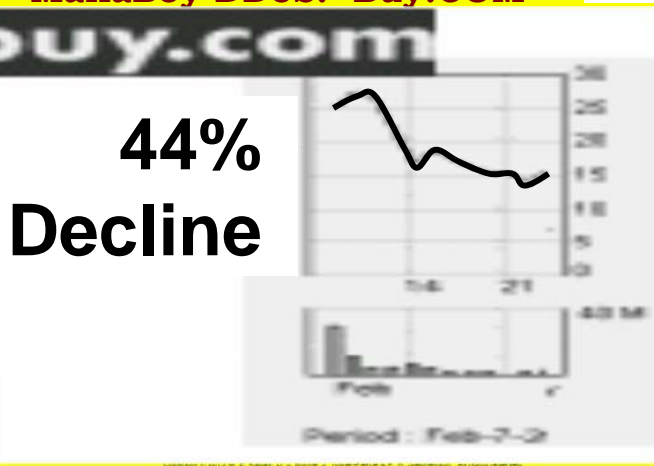
MafiaBoy DDoS: eBay Stock



MafiaBoy DDoS: Yahoo



MafiaBoy DDoS: Buy.COM



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

37

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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
 - ❑ Castlecops: anti-phishing, malware analysis, anti-spam – attacked 2007
- 2007.10.01 FBI arrested King – he threw laptop into garden before answering door
 - ❑ Contained digital evidence of his identity and crimes

38

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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*

39

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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

40

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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)

<http://www.nytimes.com/2013/08/28/business/media/hacking-attack-is-suspected-on-times-web-site.html>
or
<http://tinyurl.com/pn6srcf>

41

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

US Laws Defining Criminal Trespass with Computers



- Computer Fraud and Abuse Act
- Wire fraud
- ECPA



42

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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

43

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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

44

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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

45

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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

46

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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.

47

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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

48

Copyright © 2013 M. E. Kabay, D. J. Blythe, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

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