CRIME, ABUSE & HACKER ETHICS

D.G. Johnson, *Computer Ethics*, 2nd ed., Prentice-Hall, 1994

- Case Studies
  - Robert Morris
  - Craig Neidorf
  - The Love Bug
- Some Definitions
- Who Controls Cyberspace?
- Kinds of Abuse
- Hacker Ethics
  - Information should be free
  - Hacking shows security holes
  - Hackers aren't hurting anyone; they're just learning
  - Watchdogs for data abuse
- What Should Be Done?

CASE STUDY: ROBERT MORRIS (1988)

- Cornell CS grad student releases "worm" onto Internet
- Attack methodology
  - Password cracking
  - Sendmail attack
  - Finger daemon attack
- Worm's actions looked a lot like normal commands — intended to be hard to detect
- After infecting a system, sent a copy of itself to another system and sent a signal to a machine at UC Berkeley
- Was only supposed to infect another system once in every 15 tries, but bug made it infect 14 out of 15
- Caused serious slowdown of infected systems
- Morris tried to shut it down but failed
- Took sysadmins around the world two days to shut it down
- Did no permanent damage, but slowed systems and acquired passwords
- Morris's penalties
  - Suspended by Cornell
  - Tried in federal court under Federal Fraud & Abuse Act
  - Maximum possible sentence: 5 years prison, $250,000 fine
  - Actual sentence: $10,000 fine, 400 hours community service

CASE STUDY: CRAIG NEIDORF (1990)

- Founded online magazine *Phrack* — described legal & illegal hacking
- Law enforcement used *Phrack* many times as evidence against hackers
- Neidorf caught with a document about "Enhanced 911"
- Evidence presented to federal grand jury
- Neidorf interrogated
- Grand jury charges him with
  - Wire fraud
  - Computer fraud
  - Transporting stolen goods valued at $5,000+
- Additional wire fraud charges added later, computer fraud dropped
- Maximum possible sentence of final 10 charges: 65 years in prison
- Government's claims
  - E911 document owned by BellSouth
  - Highly sensitive
  - Worth $23,900
  - Anyone that had the file could disrupt 911 service
  - Document stolen by another hacker to publish in *Phrack*
- Outcome: E911 document shown to be
  - not highly sensitive
  - not secret
  - in public domain
- All charges dropped

CASE STUDY: LOVE BUG (2000)

- Sent in an e-mail around May 10 2000
- Subject: "I LOVE YOU" with attached document "LOVE-LETTER-FOR-YOU"
- Spread around the world in 2 hours
- Sent to roughly 84 million people, of which 2.5-3 million were affected
- "Trojan horse:" attack masquerading as an innocuous gift
- Inspired many copycat viruses
- Attack methods
  - Deleted or moved files around, especially JPEG images and MP3 music
  - Raided Microsoft Outlook Express address book and forwarded itself
  - Primarily affected systems running MS Windows
- Costs
  - Slowed Internet
  - $10 billion in lost work hours
  - Destroyed thousands of files
  - Shut down Belgian ATMs
  - Many companies (including Microsoft) and government agencies (including US Congress & UK Parliament) had to shut down their mail servers
  - Infected 80% of US federal agencies, including classified systems
- Traced to Onel de Guzman
  - Student at Amable Mendoza Aguiluz Computer College, Manila, Philippines
  - Charged with theft
  - Maximum possible sentence: 20 years in prison

`http://www.time.com/time/magazine/articles/0,3266,44514,00.html`
`http://www.pcworld.com/pcwtoday/article/0,1510,17497,00.html`

SOME DEFINITIONS

- *Cyberspace*: the collection of computers that communicate with each other
- *Internet*: the collection of computers that communicate with each other via the *Internet Protocol*
- *Hacker*
  - Originally (and to some people today): computer enthusiast — someone who stays up all night programming
  - Today: someone who breaks into other people's computers (sometimes *Cracker*)
- *Software Pirate*: makes unauthorized copies of software — sometimes distributes or even sells them
- *Virus*: a small piece of machine code that makes unwanted copies of itself into "host" programs
- *Worm*: a program that runs independently and can travel from machine to machine across a network

WHO CONTROLS CYBERSPACE?

- Who owns cyberspace?
- Who should have access to cyberspace?
- What is authorized access? Unauthorized?
- What constitutes abuse?
- What is criminal behavior in cyberspace?
- First Amendment?
- Do private property laws apply? Should they?
- Do **intellectual** property laws apply? Should they?

KINDS OF ABUSE

- *Unintentional*: accidentally gaining access or using resources
- *Intentional*: setting out to gain access or use resources
- How much does this distinction matter?
- *Abuse for Fun*: hacking just for the thrill of it
- *Abuse for Gain*: fraud, blackmail, theft, etc.
- How much does this distinction matter?

HACKER ETHICS

- Hackers generally give the following explanations
  - Information should be free.
  - Hackers help sysadmins by demonstrating security holes.
  - Hackers are doing no real harm.
  - Hackers are watchdogs for abusive misuse of data.

INFORMATION SHOULD BE FREE

- If information were free, there'd be no need for intellectual property, data security, passwords, etc.
- Some possible benefits of information being free:
  - Availabilty of information makes decision-making easier
  - Large pool of possible users of information fosters competition
  - Fairer to people who, through no fault of their own, can't afford to pay for information (e.g., public libraries)
- Some possible costs of information being free:
  - Utilitarian: why should I generate information if I don't get the benefit of it (trade secrets)?
  - Information about you could be used against you
  - National security

HACKING SHOWS SECURITY HOLES

- Pro:
  - If hackers weren't hacking, sysadmins wouldn't do much about security, in which case other hackers would have an easier time getting in.
- Could there be non-hacking ways to find security holes?
- Con:
  - Is it okay to break into someone's house to show that their locks don't work?
  - Hacking causes sysadmins to spend time chasing hackers: expensive

HACKERS AREN'T HURTING ANYONE; THEY'RE JUST LEARNING

- Plenty of hackers have caused harm, but many don't
- Is non-physical harm really harm?
- Can hackers cause physical harm?
- Is hacking the only way to learn about computers?
  Is it a good way? The best way?
- Is hacking the only way to learn about computer **security**?
  Is it a good way? The best way?

WATCHDOGS FOR DATA ABUSE

- Breaking in to corporate and government systems makes it possible to keep an eye on them and to spot instances of abuse. Examples?
- Hackers protect the public when the authorities won't — sometimes even **from** the authorities.
- Is this a good way to provide this kind of protection?
- Who gets to decide what constitutes data abuse?

WHAT SHOULD BE DONE?

- Legislation
  - Computer Fraud & Abuse Act (1986) outlaws knowingly/ intentionally accessing a computer without authorization
    - from any US government organization, or
    - to get info about national defense, foreign relations, nuclear secrets, with the intent to use the info against the US or to help another country, or
    - to get financial data from a financial institution, or
    - to get anything of value in order to defraud, or
    - destroying a federal computer's information worth over $1,000, or
    - trafficking in passwords if it affects interstate commerce.
- Good Neighbor Conventions
  - If you detect someone breaking into **someone else's** computer, you inform them and help them fix the problem.
  - If you detect someone using your system to break into others, you shut them down (and maybe prosecute or sue).
  - If someone isn't a good neighbor, you can refuse connections from them.
- Education: what can we teach people about the ethical issues that hacking brings up?