CS-4920: Lecture 4
Legal Issues and HIPAA

- Reading: None
- Today's Outcomes:
  - Identify the types and targets of computer crime
  - Summarize the major types of attacks performed by cyber criminals
  - Understand the context of the computer in the legal system
  - Appreciate the complexities of intellectual property law
  - Discuss the issues surrounding computer security and privacy rights
  - Articulate the challenges of computer forensics
  - Discuss the major provisions of HIPAA

Ref.: Merkow and Breithaupt

1

Internet Crime: Reported

- Continue to be elusive to quantify
- 2005 FBI Report:
  - $130**M** ***reported*** by 639 respondents
  - Virus, unauthorized access, info theft dominated
- 2011: FBI IC3 (Internet Crime Complaint Center) Report
  - $525**M** ***reported*** by 114,908 complainants reporting loss
    - $600 median, $4,573 average

2

Internet Crime Losses: Total?

- Extrapolation to entire US and world is problematic
  - Underreporting, mandatory reporting, liability
- $1**T** total loss estimate considered absurd by experts
  - Maass, Peter and Megha Rajagopalan. Does Cybercrime Really Cost $1 Trillion?. ProPublica, 2012-08-01. [https://www.propublica.org/article/does-cybercrime-really-cost-1-trillion/]
- $100B/y total US loss is a currently accepted estimate, highly uncertain
  - Siobhan Gorman. Annual U.S. Cybercrime Costs Estimated at $100 Billion. Wall Street Journal, 2013-07-22. [http://online.wsj.com/news/articles/SB10001424127887324328904578621880966242990]
  - What's the cost of IP that probably can't be used? (Lack of expertise?)
  - Key components:
    - Intellectual-property loss
    - Direct losses because of cybercrime
    - Loss of sensitive business information
    - Opportunity costs
    - Reputational impact

3

Why aren't incidents reported?

- FBI, 2005
  - http://www.usdoj.gov/criminal/cybercrime/FBI2005.pdf
  - 43% Negative publicity would hurt stock/image
  - 33% Competitors would use to their advantage
  - 16% Civil remedy seemed best
  - 16% Unaware of law enforcement interest
- 2012 Report / expert thinking
  - http://www.zdnet.com/unreported-cyberattacks-not-just-due-to-reputation-concerns-2062304140/
  - Lack of resources / skill / knowledge
  - Lack of process / responsible party
  - Solution: guarantee privacy, fines for non-reporting?, ...

4

Major Categories of Computer Crimes

- Military and intelligence attacks
  - Including police files
- Business attacks
- Financial attacks
- Terrorist attacks
- Grudge attacks
- Thrill attacks

according to CISSP (Certified Information Systems Security Professional)

5

Types of Crimes Committed

- (Distributed) Denial of Service (DoS) attacks
  - Yahoo! Down over 3 hours in 2/2000
  - Attacks continued for over 2 days; affected eBay, Amazon, ETrade, others
- Rogue code (Trojan horses, email attachments, etc.)
- Software piracy
- Social engineering (leading to unauthorized access)
- Dumpster diving (primary cause of ID theft)
- Spoofing of IP addresses
  - False source address, also DNS cache poisoning
- Emanation eavesdropping
  - Recall TEMPEST, industry of shielding equipment used by DOD labs, US embassies, ...
- Embezzlement (theft of money using software and databases)
- Information warfare
  - Attacks on governments to gain military or economic advantage

6

Intellectual Property Law: Copyrights

- Exclusive rights to a particular expression of an idea, not the idea itself
- In US, life of author + 70 years; 95 years for corporate works
- Includes software, audio recordings, and television broadcasts
- Fair use exceptions: 4 legal factors, but generally allows exceptions for criticism, comment, and education

7

IP Law: Patents – Background

- Exclude others from using an invention
  - In exchange for public disclosure
- Term
  - In US 20 years from filing
- International issues
  - US now (2013) on first-to-file, like most of the world
  - Trend toward harmonization; major international effort begun in 2012
- Original focus on world physical processes, manufacturing, and machinery
  - "Software patent" not legally defined
  - Debate over whether software patents encourage/discourage innovation
  - US: Cannot patent mathematical formulas for algorithms
    - But, can patent a particular application of an algorithm
  - EU: Cannot patent "computer programs" unless it can cause a "further technical effect" beyond what is inherent to HW/SW interaction
  - Confusing? Consult a patent attorney…

8

IP Law: Software Patents

- Through 1970s, USPTO would not grant patents if the invention required a computer
- Many US Supreme Court cases in early 1980s
- New PTO guidelines in 1990s, allow certain software patents
- Amazon "one-click" patent, injunction against Barnes and Noble
  - Overturned in 2001

9

IP Law: Trademarks

- "any word, name, symbol, or device, or any combination thereof"
- Purpose: identify source
- Two elements (jurisdictions may require either or both)
  - Use
  - Registration

10

IP Law: Trade Secrets

- No legal protection
- Employees may have fiduciary responsibilities to protect
- No public disclosure required
- Examples
  - Formula for drink, chemical
  - Algorithms in software
- An area of debate
  - When does an idea manifested in software move from IP law protection to the public domain?

11

International Privacy Issues

- US laws more fragmented (by industry) than the EU's
- EU's Data Protection Directive, Updated 2012
  - Notice: of collection
  - Purpose: use limited to stated purpose
  - Consent: needed for further disclosure to 3rd parties
  - Security
  - Disclosure: of who is collecting
  - Access: by the individual: correction rights
  - Accountability: of collectors by subjects
  - US Dept. of Commerce: Safe Harbor Privacy Principles for US companies to meet minimum EU privacy controls

12

Computer Forensics

- Investigating crimes committed with computers
- A large field unto itself – escalation of sophistication of criminal / investigator
- Various certification regimes, tend to focus on
  - Successful litigation based on irrefutable computer evidence
  - Adversaries are skilled at covering tracks
  - Time is of the essence (overwritten files, contamination of evidence)
  - Volatile data / RAM content recovery

13

HIPAA

- 1996 Health Insurance Portability and Accountability Act
  - Final rule with standards published February, 2003 in Federal Register
  - Protect confidential healthcare information
  - Improved security standards
  - Federal privacy legislation
  - Requirements for storing and transmitting information
  - Address confidentiality, integrity, and access
  - Guidelines for risk analysis, awareness training, audit trial, disaster recovery plans, and information access control and encryption

14

3 HIPAA Areas

- Administrative safeguards – document and implement procedures in 12 areas, including
  - Document policies and procedures for employees with access to protected health information, including training
  - Manage selection, development, and use of security controls
  - Internal audit
  - Chain of trust with adjacent parties (exchanging data)
  - Security features for initially clearing personnel
  - Termination procedures
  - Risk assessment

15

3 HIPAA Areas

- Physical safeguards
  - Identify a single responsible person
  - "Need to know" clearances
  - Securing work stations
  - Identify verification procedures
  - For systems, buildings, and equipment
  - Against natural and environment hazards and unauthorized intrusions
- Technical security services and mechanisms
  - How to protect stored information, access to data, and data transmissions

16

References

- *General*
  - *Information Security: Principles and Practices*, by Mark Merkow and Jim Breithaupt, ISBN 0131547291, Prentice Hall, 2006. (Chapter 7, Appendix E)
- Specific
  - DNS Cache Poisoning
    - http://en.wikipedia.org/wiki/DNS_cache_poisoning

17