Law and Security

CS461/ECE422

Computer Security I

Fall 2009

Overview

- Law and privacy
- Cybercrime
- Laws Affecting Computer Use

Reading Material

- *Secrets of Computer Espionage: Tactics and Countermeasures*, Joel McNamara, Chapter 2. On compass.
- CyberLaw web course from DoD.
  - http://www.cs.uiuc.edu/class/fa06/cs498sh/cyberlaw

Motivation

- Need to understand legal environment
  - Protect self/organization
    - From law suits
    - From tainted evidence
    - From attackers
  - Understand personal rights and obligations
- Caveat: I am not a legal professional...

Intellectual Property

- Desire to protect your creations from copycats
  - Copyrights
  - Patents
  - Trade secrets

Copyright

- Protect a particular "expression" of an idea
  - Original work in tangible medium
  - A particular song, arrangement, performance
  - Not the idea of a song, or a style of performance
  - Cannot copyright "Jazz music". Can copyright a particular jazz song, arrangement, etc.
- You can buy a copy and do what you want with it
  - Fair Use
  - First sale

Copyright Software and Digital Content?

- Originally concern about whether it was "tangible"
  - Amended in 1980 explicitly include software
- Digital Millennium Copyright Act (DMCA)
  - Digital objects can be copyrighted (SW, music, video)
  - Disabling copyright protection is crime
    - Can impact security research negatively
- Still not completely satisfying

Patents

- Protect inventions
  - Concrete designs of implementing particular ideas
  - Does not protect “laws of nature”
- Invention must be novel
  - First inventor gets the patent
  - Must be non-obvious to a person skilled in the field

Software Patents?

- Originally confusion about whether algorithms were “laws of nature”
  - Court case in 1981 decided for software patents
- Now software patents accepted
  - Quality can be somewhat dubious
  - Process still geared toward creation of widgets
  - A lot of work and expense to get patent and protect it

Trade Secret

- Register the fact that you have a secret
  - Don't advertise your secret sauce
- Protects against theft
- But not from reverse engineering

Tension between Privacy and Security

- How to trade off privacy for security?
  - *They who would give up an essential liberty for temporary security, deserve neither liberty or security* – Benjamin Franklin
- Relevant laws and technologies
  - 4th amendment
  - Wiretapping and Carnivore
  - Patriot Act
  - Key Escrow/DES
  - Freedom of Information Act

4th Amendment

- Fundamental privacy protection
  - The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Four Lanes of the Road

- CyberLaw course identifies four classes of investigators
  - Service Provider
  - Law Enforcement
  - Intelligence
  - War Fighter
- Laws affect them differently

USA PATRIOT Act (USAPA)

- Covers many things
- In our scope, augments or clarifies previous laws addressing electronic privacy
- Acronym
  - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism

Wiretapping

- Can wiretap only for "serious" crime
  - Wiretap act established in 1968
  - Set of serious crimes has grown, false info on student loan applications?
- Require court orders
  - Pen Registers and Tap-and-trace devices only capture "header" information, e.g., dialed numbers but not conversation
  - Full wiretap also captures content
  - Must demonstrate probable cause for full wiretap
- Wiretapping reports
  - http://www.uscourts.gov/library/wiretap.html

Electronic Wiretapping

- Electronic Communication Privacy Act of 1986 (ECPA)
  - Expands Wiretap Act to include electronic communications
- Three exceptions that don't require court authorization
  - Individual can monitor communication resulting from a break in on her computer
  - Banner that alerts computer is private implies consent to monitoring
  - Monitor to prevent misuse of system (by non-govt entity)
- USAPA said only a single court jurisdiction needed to be involved in issuing warrants

Electronic Search

- Stored Communications Act of ECPA
- Covers privacy of stored electronic data
- Requires search warrant to access data like: e-mail, voice-mail
- Two exceptions
  - Communication provider access
    - Can ask govt to help (USAPA)
  - Implied consent if supported by public policy
- Search warrant instead of wiretap implies stored data is easier to access. (USAPA)

Ensuring Wiretap Availability

- Communications Assurance for Law Enforcement Act of 1994 (CALEA)
  - Requires that telecommunication carriers use equipment that is compatible with wiretapping
  - Enforced by FBI group
  - Expensive to comply with
    - Estimated telcos will spend 0.5 to 2.7 billion dollars to comply over 5 years.

CALEA Expansions

- Recent FCC expansions
  - IP telephony must be CALEA compliant if server-oriented
    - Vonage, yes. Skype, no.
  - Expanded definition of service provider to include Universities
    - 2006 ruling confirms that Universities must comply but private network communication is exempted (e.g., staying within UIUC network)

Carnivore/DCS-1000

- FBI's program for Internet wiretaps
  - Can be tuned to track communication for specific user
  - Operate as content wiretap or trap and trace
    - Run in "tap and trace" mode. Get more stringent "content" court order if anything looks interesting
  - Gained public scrutiny in 2000
  - Software not available for public analysis
    - IIT review released
- Concerns that Carnivore really tracks all information not just the targeted user
  - Over-collection bug
  - Contaminates investigations.
    - 2002 al Qaeda investigation

Foreign Intelligence Surveillance Act (FISA)

- Addresses intelligence community instead of law enforcement
  - Generally another country is involved
- Info can be used in criminal courts with restrictions
- Separate court reviews requests

USAPA extensions to FISA

- Roving wiretaps
  - Specify target instead of phone number or type of communication
  - May over monitor to gather right data, e.g. Library
- Reduced Burden of Proof for Pen register
  - Can use on non-citizen simply to further investigation
  - Citizens protected by First Amendment...
    - http://www.usatoday.com/news/washington/2006-05-1

FISA and the War fighter

- Do FISA restrictions apply to the war fighter?

Computer Crime

- Historically difficult to prosecute
  - Lack of computer expertise
  - Laws referred only to the physical
  - Example: computer break in case that had to be stated in terms of lost computer time instead of lost data
- Use of the computer varies in criminal cases
  - Computer is the source of the crime, e.g., theft
  - Computer is means used to commit crime, e.g., net bots
  - Computer incidental to the crime, .e.g, computer was used to send email discussing crime

Computer Fraud and Abuse Act (CFAA) of 1986

- Criminalize unauthorized access to "protected computers"
  - Federal computers
  - Computers owned by large financial institutions
  - Computers user for communication or interstate commerce
    - Pretty much any computer on the Internet
    - USAPA includes foreign computers if they affect interstate commerce
- Criminalizes
  - Computer extortion, Computer Fraud, Theft of financial information, trafficking in passwords, transmitting malware.
- Maximum penalty of 20 years and $250,000 fine
  - Must cause at least $5,000 damage
  - Robert Morris of the original worm sentenced to 400 hours community service and $10,500

Economic Espionage Act of 1996

- Addresses theft of trade secrets
  - FBI can be involved in a foreign government is suspected
  - Redefines “goods, wares, or merchandise” to include company's “proprietary economic information”.

International Law

- Most western countries have similar laws
  - E.U. Data Protection Act in fact leads in personal privacy
- Difficulty in enforcing computer crime now
  - Attackers generally bounce through multiple countries
  - Look for talks from NCSA or CITES people
- French restrictions on Encryption
  - Illegal to use encryption in France until the late 1990's
  - Now requires registration and key escrow
  - Similar constraints in China and India
- China laws against speech causing civil unrest
  - Bad press against Google, Yahoo, Cisco, Microsoft and others
  - E.g., "democracy" and "freedom" gets no hits on the Chinese version of Microsoft's portal

Cryptography

- Until 1998, US had stringent restrictions on export of strong encryption
  - Cryptography as munitions
  - National Security
  - PGP source and "Warning: this T-shirt may be a controlled munition", http://www.cypherspace.org/adam/shirt/
- In 1996 US government offered to reduce export restrictions for escrow encryption
  - Clipper chip, Capstone, Forezza
  - Encryptions algorithms not fully explained
- Earlier details of reasons for DES not fully explained
  - Assumed NSA changed design for a backdoor

Secure Non-National Security Government Computers

- Federal Information Security Management Act of 2002 (FISMA)
  - Direct secure operation of computer systems not associated with national security
  - Director of the Office of Management and Budget (OMB) to oversee compliance with NIST standards
- Clinger-Cohen 1996 or Information Technology Management Reform Act (ITMRA)
  - Government must shop and compare when buying technology

Securing Computers for National Security

- National Security Directive 42 (NSD-42) 1990
  - Securing computers used for national security
  - Created Committee on National Security Systems (CNSS), an inter-agency group
    - Creates security course requirements among many other things.
  - Secretary of Defense in charge for strategy, vision, etc.
  - NSA Directory to take care of the technical details.

Industry Pressure on Compliance

- Three major regulations:
  - Sarbanes-Oxley Act (SOA or SOX)
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA)
- Compliance – providing assurance that controls are in place and effective.
- Not sufficient to just implement security services – must demonstrate continual control and management involvement.

Gramm-Leach-Bliley Act of 1999

- Requires financial institutions to protect confidentiality of customers' nonpublic personal data
  - "Customer Records"
  - Social Security, Drivers License, Birthdate
  - Credit Card Numbers
  - Loan and Account numbers
- Authorized federal agencies (including SEC and FDIC) to work out the specific regulations
- Specifies a point employee, risk assessments, regular tests, and process for updating security plan

Health Insurance Portability and Accountability Act of 1996

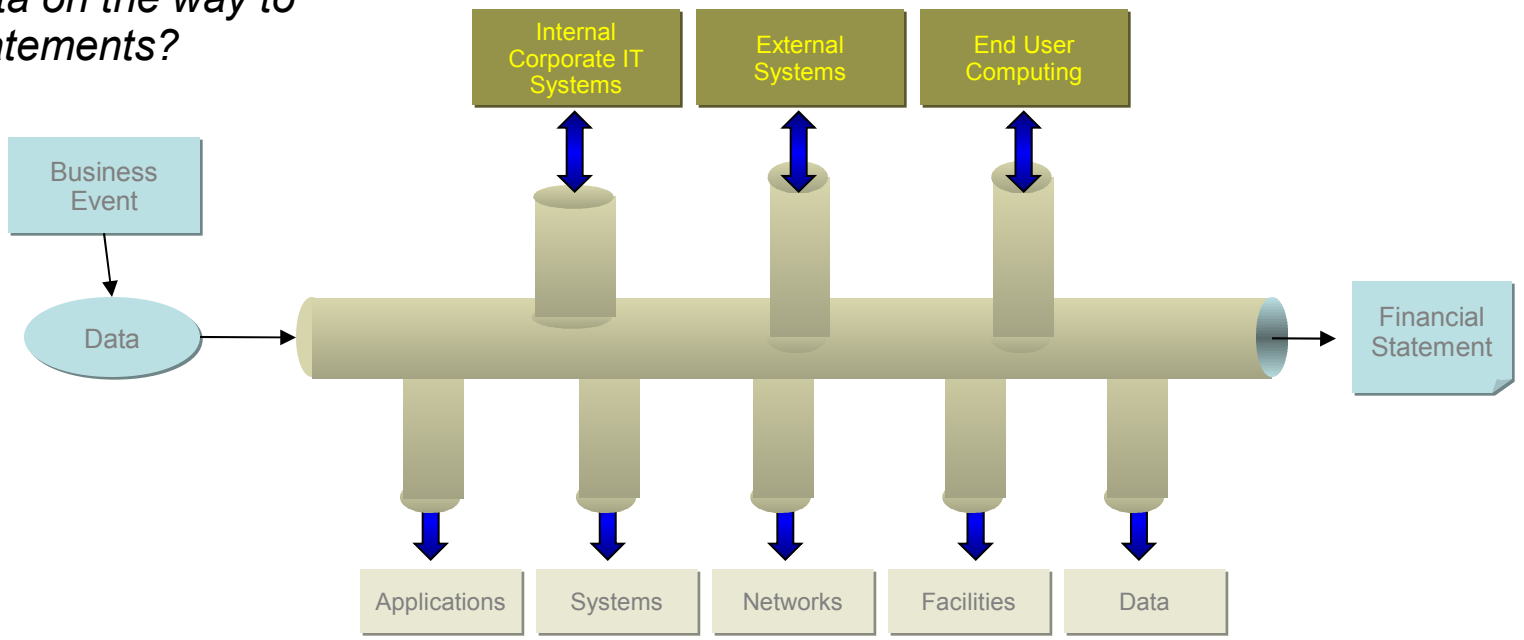
- Requires health-oriented companies to take reasonable safeguards to ensure the integrity and confidentiality of individually identifiable health information
  - Claims or equivalent encounter information
  - Payment and Remittance Advice
  - Claim Status Inquiry/Response
  - Eligibility Inquiry/Response
  - Referral Authorization Inquiry/Response
- Security of Health and Human Services in charge
- Drove many technology changes in the health sector

Sarbanes-Oxley Act of 2002 (SOX)

- Response to Enron
  - Requires companies to produce annual reports on internal financial controls
  - Directed by SEC
- Cost of compliance
  - Heavy auditing requirements
  - Lack of clarity early on concerned many companies
  - Some companies de-listed rather than comply

SOX Tracking Information Flows

What can happen to the data on the way to statements?



Slide from Jan Hertzberg, Grant Thornton, Inc.

SOX General IT Controls

- Implementation Lifecycle
  - Acquire or Develop
  - Authorized Requirements
    - Include Security Considerations
    - Application Specific Controls
    - Operating Environment Controls
  - User Acceptance Testing
- Formal Change Management Process for:
  - Application Programs
  - Operating Environment
  - Infrastructure Components
  - Regular and Emergency Chan

SOX General IT Controls (2)

- Incident Reporting
  - Monitoring, Logging, Tracking to Closure
  - Defined Process for Management Reporting
- System Infrastructure Audit
  - Includes FW, Routers, Switches, etc.
  - Examine settings on devices
  - Perform periodic vulnerability testing
    - e.g., Nessus
- Corporate Security Policy
  - High Level Policy Statement (example)
- Non-Repudiation Services

Outsourcing

- A general problem with these business requirements
  - How do you ensure that outsourcing unit treats your data appropriately? Enforces appropriate constraints?
  - Example of identity theft
  - Tax return example
    - http://www.outsourcing-offshore.com/opi.html

Key Points

- Laws and policy describe security and privacy intents
- Laws cover a range of computer issues
  - Intellectual Property
  - Government security enforcement
  - Computer crime
  - Computer investigation
- Understanding laws important
  - Many laws written without sufficient technical review
  - Impacts you or your company
  - Large societal implications