

Computer Security

CS 426

Lecture 28

Computer Crime:
Laws defining aspects of crime against or using
computers



Center for Education and Research
in Information Assurance and Security

Elisa Bertino
Purdue University
IN, USA
bertino@cs.purdue.edu

How is computer crime different than
other crimes ?

Why current laws are not sufficient ?

- Tangible vs. non-tangible
- Original evidence
- Loss of confidentiality, integrity, privacy
- Value of data
- Introduction and acceptance of computer terminology in law
- A computer can perform many roles in the crime

- Why computer crime is difficult to prosecute?

- Lack of understanding
- Lack of physical evidence
- Lack of recognition of assets
- Lack of political impact
- Complexity of case
- Age of defendant

Examples of Statutes

- U.S. Computer Fraud and Abuse Act 1984
- U.S. Economic Espionage Act
- U.S. Electronic Funds Transfer Act
- U.S. Freedom of Information Act
- U.S. Privacy Act 1974
- U.S. Electronic Communication Privacy Act 1986
- Gramm-Leach-Bliley 1999 - piracy of data for customers of financial institutions
- HIPAA 1996
- USA Patriot Act
- CAN SPAM Act
- California Breach Notification 2003
- Identity Theft Enforcement and Restitution Act

U.S. Computer Fraud and Abuse Act

- Knowingly accessing a computer without authorization in order to obtain national security data
- Intentionally accessing a computer without authorization to obtain:
 - Information contained in a financial record of a financial institution, or contained in a file of a consumer reporting agency on a consumer.
 - Information from any department or agency of the United States
 - Information from any protected computer if the conduct involves an interstate or foreign communication

U.S. Computer Fraud and Abuse Act

- Intentionally accessing without authorization a government computer and affecting the use of the government's operation of the computer.
- Knowingly accessing a protected computer with the intent to defraud and there by obtaining anything of value.

U.S. Computer Fraud and Abuse Act

- Knowingly causing the transmission of a program, information, code, or command that causes damage or intentionally accessing a computer without authorization, and as a result of such conduct, causes damage that results in:
 - Loss to one or more persons during any one-year period aggregating at least \$5,000 in value.
 - The modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals.
 - Physical injury to any person.
 - A threat to public health or safety.
 - Damage affecting a government computer system.
- Knowingly and with the intent to defraud, trafficking in a password or similar information through which a computer may be accessed without authorization.

HIPPA

- Title I of HIPAA protects **health insurance** coverage for workers and their families when they change or lose their jobs.
- Title II of HIPAA, known as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. It helps people keep their information private.

Gramm-Leach-Bliley

- *The Financial Privacy Rule* which governs the collection and disclosure of customers personal financial information by financial institutions. It also applies to companies, regardless of whether they are financial institutions, who receive such information.
- *The Safeguards Rule* requires all financial institutions to design, implement and maintain safeguards to protect customer information. The Safeguards Rule applies not only to financial institutions that collect information from their own customers, but also to financial institutions such as credit reporting agencies that receive customer information from other financial institutions.

California Breach Notification

- State government agencies as well as companies and nonprofit organizations regardless of geographic location must notify California customers if personal information maintained in computerized data files have been compromised by unauthorized access.
- California consumers must be notified when their name is illegitimately obtained from a server or database with other personal information such as their Social Security number, driver's license number, account number, credit or debit card number, or security code or password for accessing their financial account.

International Agreements/Acts

- Council of Europe Agreement on Cybercrime 2001 (US, Canada, Japan, 22 European countries)
- E.U. Data Protection Act
- Restricted content

Computer Crime: Laws and ethics

What is the difference between laws and ethics?

- > Most of the time laws are written, approved, and then enforced by the level of government where they were written.
 - For example, a State law is enforced by the state. A Federal law is enforced by the Federal Government.
 - In other words, State Laws and Government Laws go through a process to get approved, written into law, and then are enforced.
- > Ethics are like rules of conduct.
 - For example, physicians have unwritten ethical rules or practices that they adhere to just because it's the right thing to do. They have the responsibility to take care of you to the best of their ability. It's ethically correct for a physician to do his best to help a patient with his/her malady, but it is not a law that he has to.
 - If a physician is unable to help the patient with his/her problem he has an ethical responsibility to refer the patient to a specialist, but there is not a law saying that he has to do that.

Case: Wiretapping

- A group of researchers from the University of Colorado and University of Washington conducting a research project set up a TOR node (as in Tor anonymous network) and logged all the communication which was then accidentally left on a publicly accessible server
- Is their behavior ethical?
- Is their behavior legal?

Case: Wiretapping

- They could face both civil and criminal penalties for a research project
- They could also face up to 5 years in jail for violating the Wiretap Act
- The researchers neither sought legal review of the project nor ran it past their Institutional Review Board
- The Electronic Frontier Foundation, which has written a legal guide for Tor admins, strongly advises against any sort of network monitoring

Case: Pirate Bay

- Hosting of lists of available data subjected to copyright
- Sites hosted in Sweden
- Is their behavior legal?
- Is their behavior ethical?

- If they assisted in copyright infringements, how about the ISPs ?

Case: Privacy Rights

- Donald works for the county records where he accesses files of property tax records. For a scientific study, Ethel has been given access to the numerical portion, but not the names.
- Ethel finds the information, but she needs the names and addresses of those people and asks Donald to retrieve them for her so she can contact them for more information and permission for further study.
- Should Donald release the name?

Case: Ownership of Programs

- Who owns the programs: the programmer, the employer, the manager, or all?
- Greg is a programmer working for a large aerospace firm Star, which works for many government contracts; Cathy is Greg's supervisor. Greg is assigned to program various simulations.
- Greg writes some programming tools; these are not assigned tasks for Greg, he writes them at home, in the evening, on his own computer, but uses them at work.

Case: Ownership of Programs

- Greg decides to market these programming tools for himself. Star management tell Cathy to tell Greg that he has not right to market these products since in his contract says that all the inventions developed while working for Star belong to Star. Cathy does not agree, also asks for a copy of the software
- Cathy leaves Star and goes to work for Purple (competitor of Star), she gives the copy of Greg's software to the people that work with her. For her success (productivity due to this software) Cathy receives a bonus. Greg finds out and he contends that because the software was deemed to belong to Star and because Star worked on government contracts, the products were in the public domain and belonged to one in particular.

Case: Ethics of Hacking and Cracking

- Goli is a computer consultant, independently wealthy she does not need to work, so she uses her time to test the security of systems:
 - She aggressively attacks commercial products for vulnerabilities
 - She probes accessible systems on the Internet and when she finds problems she contacts the owner to offer her services to repair the problems
 - She plants small programs to slow performance in the web sites of pastry shops that do not use enough butter in their products
 - Which of her actions are ethical, if any?

Code of Ethics

- Many professions have established professional societies, which have adopted codes of conduct.
 - American Medical Association (AMA)
 - American Bar Association (ABA)
- Computing professional societies
 - The Association for Computing Machinery (ACM)
 - The Institute for Electrical and Electronics Engineers – Computer Society (IEEE-CS)

ACM Code of Ethics and Conduct

- 1.1 Contribute to society and human well-being.
- 1.2 Avoid harm to others.
- 1.3 Be honest and trustworthy.
- 1.4 Be fair and take action not to discriminate.
- 1.5 Honor property rights including copyrights and patent.
- 1.6 Give proper credit for intellectual property.
- 1.7 Respect the privacy of others.
- 1.8 Honor confidentiality.

As an ACM computing professional I will ...

- 2.1 Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work.
- 2.2 Acquire and maintain professional competence.
- 2.3 Know and respect existing laws pertaining to professional work.
- 2.4 Accept and provide appropriate professional review.
- 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
- 2.6 Honor contracts, agreements, and assigned responsibilities.
- 2.7 Improve public understanding of computing and its consequences.
- 2.8 Access computing and communication resources only when authorized to do so.

As an ACM member and an organizational leader, I will

- 3.1 Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities.
- 3.2 Manage personnel and resources to design and build information systems that enhance the quality of working life.
- 3.3 Acknowledge and support proper and authorized uses of an organization's computing and communication resources.
- 3.4 Ensure that users and those who will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated to meet requirements.
- 3.5 Articulate and support policies that protect the dignity of users and others affected by a computing system.
- 3.6 Create opportunities for members of the organization to learn the principles and limitations of computer systems.

As an ACM member I will

- 4.1 Uphold and promote the principles of this Code.
- 4.2 Treat violations of this code as inconsistent with membership in the ACM.