

# Crime

CSE 312 – Legal, Social, and Ethical Issues in  
Information Systems

Stony Brook University

<http://www.cs.stonybrook.edu/~cse312>

# Ch 5: Crime

## 5.1 Introduction

## 5.2 Hacking

5.2.1 What is “Hacking”?

5.2.2 Hacktivism, or Political Hacking

5.2.3 Hackers as Security Researchers

5.2.4 Hacking as Foreign Policy

5.2.5 Security

5.2.6 The Law: Catching and Punishing Hackers

## 5.3 Identity Theft and Credit Card Fraud

5.3.1 Stealing Identities

5.3.2 Responses to Identity Theft

5.3.3 Biometrics

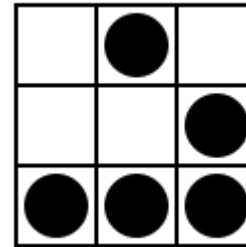
## 5.4 Whose Laws Rule the Web?

5.4.1 When Digital Actions Cross Borders

5.4.2 Libel, Speech, and Commercial Law

5.4.3 Culture, Law, and Ethics

5.4.4 Potential Solutions



# Hacking

- Intentional, unauthorized access to computer systems
- The term has changed over time
- Phase 1: The joy of programming
  - Early 1960s to 1970s
  - Hacking was a positive term
  - A "hacker" was a creative programmer who wrote elegant or clever code
  - A "hack" was an especially clever piece of code
  - "Hacking" still sometimes has the early meaning of clever programming that reflects a high level of skill and that circumvents limits (*Hackathons: sprint-like event in which programmers collaborate intensively on software projects*)

# Hacking

- Phase 2: 1970s to mid 1990s
  - Hacking took on negative connotations
  - Breaking into computers for which the hacker does not have authorized access
    - A Russian man used stolen passwords to steal \$400,000 from Citicorp and transferred \$11 million to accounts in other countries
      - It took 2 years to extradite him from London to US for trial
  - Still primarily individuals
  - Includes the spreading of computer worms and viruses and ‘*phone phreaking*’ (manipulating the telephone system)
  - Companies began using hackers to analyze and improve security

# Hacking

- Phase 3: The growth of the Web and mobile devices
  - Beginning in mid 1990s
  - The growth of the Web changed hacking; viruses and worms could be spread rapidly
    - The Melissa virus of 1999 infected approximately a million computers worldwide
    - In 2000, the “Love Bug,” or “ILOVEYOU” virus, spread around the world in a few hours and destroyed image and music files, modified a computer’s operating system and Internet browser, and collected passwords
  - Political hacking (*Hacktivism*) surfaced
    - They modified the U.S. Department of Justice Web page to read “Department of Injustice” in protest of the Communications Decency Act
  - Denial-of-service (*DoS*) attacks used to shut down Web sites: victims included Yahoo, eBay, Amazon, E\*Trade, Buy.com, CNN
  - Large scale theft of personal and financial information

# Hacking

- Phase 3: The growth of the Web and mobile devices
  - A new type of virus gives the person who distributed it the power to remotely control the infected computers (called *zombies*), that can now send spam, contribute to denial-of-service attacks, participate in various kinds of online advertising fraud
    - A 21-year-old California man pleaded guilty and was sentenced to almost five years in prison (the longest hacking sentence at that time, 2006) – he took over hundreds of thousands of computers (some at military sites)

# Hacking

- Is “harmless hacking” **harmless**?
  - The excitement and challenge of breaking in motivates young hackers.
  - Some claim that such hacking is harmless. Is it?
- Responding to nonmalicious or prank hacking uses resources
  - After a hacker accessed a Boeing Corporation computer, Boeing spent a large sum to verify that the intruder changed no files
- Hackers could accidentally do significant damage
  - A group of young Danes broke into National Weather Service computers, but their activities caused the Weather Service computers to slow down.
    - Serious conditions, such as tornadoes, could have gone undetected and unreported
- Almost all hacking is a form of trespass.

# Hacking

- Hacktivism, or Political Hacking
  - Use of hacking to promote a political cause
- Disagreement about whether it is a form of civil disobedience and how (whether) it should be punished
  - Is there ethical justification for such hacking?
  - Should penalties for hacktivists differ from penalties for other hackers?
- Some use the appearance of hacktivism to hide other criminal activities
- How do you determine whether something is hacktivism or simple vandalism?
  - A hacker group hacked into the Bay Area Rapid Transit (BART) system and released emails, passwords, and personal information about a few thousand BART customers to protest BART's controversial shutdown of wireless communication in several BART stations to thwart a planned protest demonstration



# Hacking

- Hacktivism, or Political Hacking
  - Are hacktivists merely exercising their freedom of speech?
  - Freedom of speech does not include the right to hang a political sign in a neighbor's window or paint one's slogans on someone else's fence
- Civil disobedience has a respected, nonviolent tradition
  - Henry David Thoreau, Mahatma Gandhi, and Martin Luther King Jr. refused to cooperate with rules they saw as unjust
  - Peaceful protestors have marched, rallied, and boycotted to promote their goals
  - Hacking is not civil disobedience

# Hacking

- Hackers as Security Researchers
  - hackers probe computer systems, most often without permission, to find security flaws as an intellectual exercise
  - They sometimes call themselves “security researchers” to avoid the now negative connotation of the term hacker

# Hacking

- “White hat hackers” use their skills to demonstrate system vulnerabilities and improve security
  - In old cowboy movies, the good guys wore white hats
- Those who use methods of questionable legality or publicize vulnerabilities before informing the system owners are sometimes called “gray hats”
  - A group called Goatse Security collected the email addresses of more than 100,000 iPad owners from an AT&T website. They notified the media about the security flaw after AT&T fixed it.
  - A security researcher discovered a major flaw in the Internet’s domain name server system. He kept the problem secret while working with several companies to develop a patch. He released the patch and "encouraged" companies to install it within 30 days by giving them a timeline of 30 days before releasing the details of hacking.



# Hacking

- Hacking as Foreign Policy

- Hacking by governments has increased

*In the 21st century, bits and bytes can be as threatening as bullets and bombs.*

—William J. Lynn III, Deputy Defense Secretary

- The first cyber attack apparently coordinated with a military attack occurred in 2008 when the Russian military moved into Georgia
  - Georgian government websites were attacked and some disabled
    - It is very likely that the Russian government was responsible
- A Chinese government-owned company sent false messages to the Internet routing system to reroute a large amount of Internet traffic from U.S. military agencies and Congress through servers in China

# Hacking

- Hackers from computers originated in China stole several terabytes of information about the design of one of the Pentagon's new and extremely expensive fighter jets
  - Announced by the deputy defense secretary in 2011
  - The *New York Times* described a theft of 24,000 Defense Department documents as “one of its worst digital attacks in history”
- Computers from a Chinese city where a major Chinese national security division is located performed a 2011 attack on the Gmail accounts of White House staffers
- Russian and Chinese hackers broke into computer networks that control the U.S. electric power grid, U.S. satellites, oil and gas companies worldwide
- Pentagon has announced it would consider and treat some cyber attacks as acts of war, and the U.S. might respond with military force.

# Hacking

- Stuxnet
  - An extremely sophisticated worm
  - Targets a particular type of control system
  - Beginning in 2008, damaged equipment in a uranium enrichment plant in Iran
  - The focus on Iran's nuclear program and the sophistication of Stuxnet led to speculation that the Israeli and/or U.S. government created it.
  - Siemens Simatic S7-300 PLC



- In 2012, journalist David Sanger published extensive research indicating that the two governments did indeed produce Stuxnet

# Hacking

- Security

- Hacking is a problem, but so is poor security.

*The fact that I could get into the system amazed me.*

—Frank Darden, a member of the Legion of Doom, which hacked the BellSouth telephone system

- Variety of factors contribute to security weaknesses:

- History of the Internet and the Web
- Inherent complexity of computer systems
- Speed at which new applications develop
- Economic and business factors
- Human nature

# Hacking

- Internet started with open access as a means of **sharing and communicating information** for research
- **The Internet was not designed for security against malicious intruders, teenage explorers, or organized criminals**
- Attitudes about security were slow to catch up with the risks.
  - Internet security expert Dan Farmer ran a program to probe the websites of banks, newspapers, government agencies for software loopholes that made it easy for hackers to invade and disable or damage the sites:
    - two-thirds had security weaknesses
    - only four sites apparently noticed that someone was probing their security
- Firewalls are used to monitor and filter out communication from untrusted sites or that fit a profile of suspicious activity.
- Security is often playing catch-up to hackers as new vulnerabilities are discovered and exploited.



# Hacking

- Competitive pressure spurs companies to develop products with insufficient thought or budget devoted to analyzing potential security risks and protecting against them
  - Databases included unencrypted credit card numbers and other security numbers read from the magnetic strips on the cards
- Retailer TJX used a vulnerable, out-of-date encryption system to protect data transmitted between cash registers and store computers on its wireless network
- More and more appliances and machinery—from microwave ovens to cars to factory machinery to heart monitors—are going online
  - An app allows a car owner to open his car from his phone
    - He sold the car, unregistered the car, but he discovered three years later he still had access to the car systems.

# Hacking

- Responsibility for Security
  - Developers have a responsibility to develop with security as a goal.
  - Businesses have a responsibility to use security tools and monitor their systems to prevent attacks from succeeding.
    - Sellers of any widely used consumer product have an ethical obligation to build in a level of safety appropriate for the general population
  - Software companies have an ethical obligation to design and implement their products so that they do not expose users to severe security threats.
  - Home users have a responsibility to ask questions and educate themselves on the tools to maintain security (personal firewalls, anti-virus and anti-spyware).
  - Government agencies that operate major infrastructure systems and defense systems have a profound responsibility for improving security

# Hacking

## The Law

- 1984 Congress passed the Computer Fraud and Abuse Act (CFAA)
  - Covers government computers, financial and medical systems, and activities that involve computers in more than one state, including computers connected to the Internet
  - Under CFAA, it is illegal to access a computer without authorization
- The USA PATRIOT Act expanded the definition of loss to include the cost of responding to an attack, assessing damage and restoring systems
  - It raised the maximum penalty in the CFAA for a first offense to 10 years
  - It increased penalties for hacking computers used by the criminal justice system or the military
  - It allows the government to monitor online activity of suspected hackers without a court order

# Hacking

- Catching hackers
  - Law enforcement agents read hacker newsletters and participate in chat rooms undercover
    - They can often track a handle by looking through newsgroup or other archives
  - Security professionals set up '*honey pots*' which are Web sites that attract hackers, to record and study
  - *Computer forensics (digital forensics)* specialists can retrieve evidence from computers, even if the user has deleted files and erased the disks
  - Investigators trace viruses and hacking attacks by using ISP records and router logs
    - David Smith, the man who released the Melissa virus, used someone else's AOL account, but AOL's logs contained enough information to enable authorities to trace the session to Smith's telephone line
    - In 2011-2012, members of Anonymous and LulzSec were arrested in several countries

# Hacking

- Penalties for young hackers
  - Many young hackers have matured and gone on to productive and responsible careers
    - Steve Wozniak created the Apple computer. But before he was building Apples, Wozniak was building blue boxes, devices that enabled people to make long-distance phone calls without paying for them.
  - Temptation to over or under punish
  - Sentencing depends on intent and damage done
  - Most young hackers receive probation, community service, and/or fines
  - Not until 2000 did a young hacker receive time in juvenile detention
    - A 16-year-old that had broken into NASA and Defense Department computers and was a member of a hacker group that vandalized government websites.

# Hacking

- Criminalize virus writing and hacker tools?
  - Security personnel and researchers must be able to possess security and hacker software to effectively do their job.
  - We saw in Chapter 3 (Freedom of Speech) that writing about how to make illegal or destructive devices, such as bombs, is not (in most cases) illegal.
    - But, the First Amendment does not protect some kinds of speech, such as inciting a riot
  - Encouraging people to commit destructive or illegal actions is generally protected by the First Amendment in situations where the listener has time to reflect and make a decision about whether to act
    - A person who reads virus code has the opportunity to decide whether to activate the virus.

# Hacking

## The Law: Catching and Punishing Hackers

- Expansion of the Computer Fraud and Abuse Act
  - The CFAA predates social networks, smartphones, and sophisticated invisible information gathering.
  - Some prosecutors use the CFAA to bring charges against people or businesses that do unauthorized data collection.
    - Is violating terms of agreement a form of hacking?

# 5.3 Identity Theft and Credit Card Fraud

- Stealing Identities (Identity Theft): various crimes in which criminals use the identity of an unknowing, innocent person
  - Use credit/debit card numbers, personal information, and social security numbers
  - 18-29 year-olds are the most common victims because they use the Web most and are unaware of risks
  - E-commerce has made it easier to steal and use card numbers without having the physical card
    - Credit card companies and other businesses bear the direct cost of most credit card fraud, but the losses lead to higher charges to consumers: individual victims might lose a good credit rating, be prevented from borrowing money or cashing checks, be unable to get a job, or be unable to rent an apartment
  - The Federal Trade Commission receives hundreds of thousands of complaints of identity theft each year



# Identity Theft and Credit Card Fraud

- Techniques used to steal personal and financial information
  - Requests for personal and financial information disguised as legitimate business communication
    - *Phishing* – e-mail
    - *Smishing* – text messaging
    - *Vishing* – voice phishing
  - *Pharming* – false Web sites that fish for personal and financial information by planting false URLs in Domain Name Servers
    - Online resumés and job hunting sites may reveal SSNs, work history, birth dates and other information that can be used in identity theft
- Thieves surreptitiously install recording devices (called *skimmers*) inside the card readers

# Identity Theft and Credit Card Fraud

- Responses to Identity Theft
  - Authentication of email and Web sites
    - Email programs, Web browsers, search engines, and add-on software (some free) can alert users to likely fraud
      - emails claiming to be from PayPal has come from hotmail.com, yahoo.com
  - Use of encryption to securely store data, so it is useless if stolen
  - In the event information is stolen, a fraud alert can flag your credit report (*fraud alert*); some businesses will cover the cost of a credit report if your information has been stolen
    - calls you for confirmation when anyone tries to open a new credit account (e.g., for a car loan or credit card) in your name
  - Unique IDs used for each transaction
  - Credit card companies run sophisticated artificial intelligence software to detect unusual spending activity

# Identity Theft and Credit Card Fraud

- Responses to Identity Theft
  - Authenticating customers and preventing use of stolen numbers
    - Activation for new credit cards
    - Retailers do not print the full card number and expiration date on receipts
    - Software detects unusual spending activities and will prompt retailers to ask for identifying information
    - Services, like PayPal, act as third party allowing a customer to make a purchase without revealing their credit card information to a stranger

# Identity Theft and Credit Card Fraud

- *Biometrics*
  - Biological characteristics unique to an individual
    - fingerprints, voice prints, face structure, hand geometry, eye (iris or retina) patterns, and DNA.
  - No external item (card, keys, etc.) to be stolen
  - Used in areas where security needs to be high, such as identifying airport personnel
  - Biometrics can be fooled, but more difficult to do so, especially as more sophisticated systems are developed
  - Even low end biometrics, like photos on credit cards, proved to be helpful

# Whose Laws Rule the Web

- When Digital Actions Cross Borders
  - The ILOVEYOU virus infected tens of millions of computers worldwide in 2000, destroying files, collecting passwords, and snarling computers at major corporations and government agencies
    - The prosecutors dropped charges against the Philippine man believed responsible
    - Should he be arrested if he comes to US?
  - Someone whose actions are legal in their own country may face prosecution in another country where their actions are illegal.
- Laws vary from country to country
  - For example, in the United States, the government may not appeal acquittals
- Corporations that do business in multiple countries must comply with the laws of all the countries involved.

# Whose Laws Rule the Web

- Yahoo and French censorship
  - Display and sale of Nazi memorabilia illegal in France and Germany
  - Yahoo was sued in French court (1999) because French citizens could view Nazi memorabilia offered on Yahoo's U.S.-based auction sites
    - Legal issue is whether the French law should apply to Yahoo auction sites on Yahoo's computers located outside of France.
    - Yahoo said the use of filters to screen out Nazi material would not suffice, because they would be less than 50% effective and could not distinguish references to Nazis in hate material from references in The Diary of Anne Frank or Holocaust memorials
    - A few companies were already using software, called *geolocation software*, to figure out where website visitors were located.
      - But people could use anonymizers
  - Acquitted because the court decided that permitting the auctions was not “justifying” the Nazi crimes

# Whose Laws Rule the Web

- Applying U.S. copyright law to foreign companies
  - A Russian company, ElcomSoft, sold a computer program that circumvents controls embedded in electronic books to prevent copyright infringement.
    - Program was legal in Russia, but illegal in U.S.
  - The program's author, Dmitry Sklyarov, was arrested when arrived in U.S. to present a talk on the weaknesses in control software used in ebooks
    - He faced a possible 25-year prison term
  - After protests in U.S. and other countries, he was allowed to return to Russia
  - The company stopped distributing the program when Adobe complained.

# Whose Laws Rule the Web

- Arresting executives of online gambling and payment companies
  - An executive of a British online gambling site was arrested as he transferred planes in Dallas. (Online sports betting is not illegal in Britain.)
    - Most of the companies' customers were in the United States, where most online gambling is illegal
    - Carruthers, facing a possible 20-year jail sentence, pleaded guilty for a lower sentence.
  - Unlawful Internet Gambling Enforcement Act (2006) prohibits credit card and online-payment companies from processing transactions between bettors and gambling sites.



# Whose Laws Rule the Web

- Libel, Speech and Commercial Law
  - Under defamation law, we can sue a person, business, or organization for saying something false and damaging to our reputations in print or in other media such as television or the Web.
  - *Libel* is written defamation; *slander* is verbal.
    - Michael Jackson won a libel suit against a British newspaper for a statement that his plastic surgeries “hideously disfigured” him.
  - In cases of libel, the burden of proof differs in different countries
    - Michael Jackson probably would not have won the suit in the United States because of freedom of speech
    - In England, people often sue newspapers, and it can be risky to publish details about business and political scandals
  - In the United States, the person who is suing has the burden of proving the case

# Whose Laws Rule the Web

- Libel law as a threat to free speech
- Libel tourism
  - Traveling to places with strict libel laws in order to sue
  - SPEECH Act of 2010 makes foreign libel judgments unenforceable in the U.S. if they would violate the First Amendment. Foreign governments can still seize assets.
- Where a trial is held is important not just for differences in the law, but also the costs associated with travel between the countries; cases can take some time to come to trial and may require numerous trips.
- Freedom of speech suffers if businesses follow laws of the most restrictive countries.

# Whose Laws Rule the Web

## Discussion Questions

- *What suggestions do you have for resolving the issues created by differences in laws between different countries?*
- *What do you think would work, and what do you think would not?*

# Culture, Law, and Ethics

- Respecting cultural differences is not the same as respecting laws
  - Where a large majority of people in a country support prohibitions on certain content, is it ethically proper to abandon the basic human rights of free expression and freedom of religion for minorities?
- Governments often claim to be protecting national culture and values when they impose controls on their citizens to maintain their own power or to benefit special interests within their country.

# International agreements

- Countries of the **World Trade Organization (WTO)** agree not to prevent their citizens from buying certain services from other countries if those services are legal in their own.
  - The WTO agreement does not help when a product, service, or information is legal in one country and not another.
- Cybercrime Treaty (Budapest Convention on Cybercrime by the Council of Europe 2001)
  - International agreement foster international cooperation among law enforcement agencies of different countries in fighting copyright violations, pornography, fraud, hacking and other online crime
  - Treaty sets common standards or ways to resolve international cases
  - It requires countries to outlaw some formally legal activities
  - The non–Council of Europe states that have ratified the treaty are Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka, and the United States.

# International agreements

- **Responsibility-to-prevent-access**

- Publishers must prevent material or services from being accessed in countries where they are illegal.
- They may be sued or jailed in those countries if they do not prevent access.

- **Authority-to-prevent entry**

- Government of Country A can act within Country A to try to block the entrance of material that is illegal there, but may not apply its laws to the people who create and publish the material, or provide a service, in Country B if it is legal there.