Computer Crime
(Class 4.2 – February 7, 2013)

CSE 3316 – Professional Practices
Spring 2013
Instructor – Bill Carroll, Professor of CSE
What We Will Cover

- Hacking
- Identity Theft and Credit Card Fraud
- Whose Laws Rule the Web
Hacking

- Intentional, unauthorized access to computer systems
- The term has changed over time
- Phase 1: The joy of programming
  - Early 1960s to 1970s
  - It 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

Phase 2: 1970s to mid 1990s

- Hacking took on negative connotations
- Breaking into computers for which the hacker does not have authorized access
- Still primarily individuals
- Includes the spreading of computer worms and viruses and ‘phone phreaking’
- 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
- Political hacking (Hacktivism) surfaced
- Denial-of-service (DoS) attacks used to shut down Web sites
- Large scale theft of personal and financial information
Hacking

Is “harmless hacking” harmless?

- Responding to nonmalicious or prank hacking uses resources.
- Hackers could accidentally do significant damage.
- Almost all hacking is a form of trespass.
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
- Some use the appearance of hacktivism to hide other criminal activities
- How do you determine whether something is hacktivism or simple vandalism?
Hackers as Security Researchers

“White hat hackers” use their skills to demonstrate system vulnerabilities and improve security.
Hacking as Foreign Policy

- Hacking by governments has increased
- Pentagon has announced it would consider and treat some cyber attacks as acts of war, and the U.S. might respond with military force.
- How can we make critical systems safer from attacks?
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
Hacking

Security

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

- Internet started with open access as a means of sharing information for research.
- Attitudes about security were slow to catch up with the risks.
- 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.
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.
- Home users have a responsibility to ask questions and educate themselves on the tools to maintain security (personal firewalls, anti-virus and anti-spyware).
Hacking

Discussion Questions

- *Is hacking that does no direct damage a victimless crime?*

- *Do you think hiring former hackers to enhance security is a good idea or a bad idea? Why?*
Hacking

The Law: Catching and Punishing Hackers

- 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
Hacking

The Law: Catching and Punishing Hackers

- 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 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
The Law: Catching and Punishing Hackers

- Penalties for young hackers
  - Many young hackers have matured and gone on to productive and responsible careers
  - 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
Hacking

The Law: Catching and Punishing Hackers

- Criminalize virus writing and hacker tools?
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?
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

Corresponding page number: 250-253
Identity Theft and Credit Card Fraud

Stealing Identities

- 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 resumes and job hunting sites may reveal SSNs, work history, birth dates and other information that can be used in identity theft
Identity Theft and Credit Card Fraud

Responses to Identity Theft

- Authentication of email and Web sites
- Use of encryption to securely store data, so it is useless if stolen
- Authenticating customers to prevent use of stolen numbers, may trade convenience for security
- In the event information is stolen, a fraud alert can flag your credit report; some businesses will cover the cost of a credit report if your information has been stolen
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
- 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
When Digital Actions Cross Borders

- Laws vary from country to country.
- Corporations that do business in multiple countries must comply with the laws of all the countries involved.
- Someone whose actions are legal in their own country may face prosecution in another country where their actions are illegal.
Yahoo and French censorship

- Display and sale of Nazi memorabilia illegal in France and Germany
- Yahoo was sued in French court 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.
Whose Laws Rule the Web

Applying U.S. copyright law to foreign companies

- Russian company 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.
- Program’s author, Dmitry Sklyarov, arrested when arrived in U.S. to present a talk on the weaknesses in control software used in ebooks.
- After protests in U.S. and other countries, he was allowed to return to Russia.

Corresponding page number: 261
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.)
- Unlawful Internet Gambling Enforcement Act 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

- Even if something is illegal in both countries, the exact law and associated penalties may vary.
- In cases of libel, the burden of proof differs in different countries.
Whose Laws Rule the Web

Libel, Speech and Commercial Law

- 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

Libel, Speech and Commercial Law

- Some countries have strict regulations on commercial speech and advertising.
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?
Potential Solutions

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.
Potential Solutions

Alternative principles

- Responsibility-to-prevent-access
  - Publishers must prevent material or services from being accessed in countries where they are illegal.

- 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.