CSE/ISE 312

Chapter 5: Computer Crime

Outline

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

What is Hacking?

- **Hacking** – currently defined as Intentional, unauthorized access to computer systems
- The term has changed over time
- Phase 1: 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 (cont.)

- 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, viruses and ‘phone phreaking’
  - Companies began using hackers to analyze and improve security

Hacking (cont.)

- Phase 3: starting the 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

Hacktivism

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?

Security vs hacking

- 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 un-trusted 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)

The Law re. Hacking

- 1984 Congress passed the Computer Fraud and Abuse Act (CFAA)
  - Covers government computers, financial and medical systems, activities that involve computers in more than one state, computers connected to the Internet
  - Outlaws hacking activities: DoS, malware, unauthorized access, fraud, impairing gov operations, public utilities
  - The USA Patriot Act expanded the definition of loss to include the cost of responding to an attack, assessing damage and restoring systems

Catching Hackers

A variety of methods for catching hackers

- Law enforcement agents read hacker newsletters and participate in chat rooms undercover
- They can often track a handle by looking through newsgroup archives
- Security professionals set up ‘honey pots’ which are Web sites that attract hackers, to record and study
- Computer forensics is used to retrieve evidence from computers for legal purposes
- Investigators trace viruses and hacking attacks by using ISP records and router logs

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

Stealing Identities

- **Identity Theft** – various crimes in which a criminal or large group uses 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 card numbers and use without having the physical card

Theft Techniques

- Techniques used to steal personal and financial information
  - Phishing - e-mail fishing for personal and financial information disguised as legitimate business e-mail
    - Smishing – text messaging. Vishing – voice phishing
  - Pharming - planting false URLs in Domain Name Servers, lead to false Web sites that fish for personal and financial information
  - Online resumes and job hunting sites may reveal SSNs, work history, birth dates and other information that can be used in identity theft

Responses to Identity Theft

- Authentication of e-mail 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
- Biometrics: biological characteristics unique to an individual – “what you are”

Protection Techniques

- 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

Whose Laws Rule the Web

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

Example Cases

- American arrested in Thailand for translating a biography of the king and posting it
- Canada bans reporting court proceeding in political scandals, if an American reported it, can he be arrested if he visits Canada?
- Yahoo vs French censorship, Nazi memorabilia
- DRM circumvention by Russian. Legal in Russia
- Arresting executives of online gambling and payment companies

Libel, Speech, 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
  - Some on public figures, some on newspapers

- Some countries have strict regulations on commercial speech and advertising

Libel law: 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 trial and may require numerous trips
- Freedom of speech suffers if businesses follow laws of the most restrictive countries

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?

Cybercrime Treaty

- 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

“Responsibility to prevent access”

- So far governments are assuming a “Responsibility to prevent access” principle:

  It is the responsibility of providers of services and information to make sure their material is not accessible in countries where it is illegal. They may be sued or jailed in those countries if they do not prevent access

Alternative Principles

- So far governments are assuming a “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.