Computer Law and Ethics, COSC-3325, Lecture 8

Stefan Andrei

Reminder of the last lecture

- Google AdWords and European Trademark Law
- Based on the paper:
  - Stefan Bechtold: Law and Technology - Google AdWords and European Trademark Law, *Communications of the ACM*, January 2011, vol. 54, no. 1

Overview of This Lecture

- Hacking
- Identity Theft and Credit Card Fraud
- Scams and Forgery
- Crime Fighting Versus Privacy and Civil Liberties
- Laws That Rule the Web

Hacking

- Hacking – currently defined as to gain illegal or unauthorized access to a file, computer, or network.
- 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 and viruses and ‘phone phreaking’ (one who gains illegal access to the telephone system);
  - Companies began using hackers to analyze and improve security.

Hacking (cont.)

- Phase 3: beginning with 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.

Hacking (cont.)

Hacktivism, or Political Hacking:

- Use of hacking to promote a political cause;
- Disagreement about whether it is a form of civil disobedience and how (or whether) it should be punished;
- Some use the appearance of hacktivism to hide other criminal activities;
- How do we determine whether something is hacktivism or simple vandalism?

Hacking (cont.)

The Law: Catching and Punishing Hackers:

- In 1986, 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;
    - The USA Patriot Act expanded the definition of loss to include the cost of responding to an attack, assessing damage and restoring systems.

Hacking (cont.)

The Law: Catching and Punishing Hackers (cont.):

- 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.

Hacking (cont.)

The Law: Catching and Punishing Hackers (cont.):

- 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 (cont.)

The Law: Catching and Punishing Hackers (cont.):

- 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.

Hacking (cont.)

The Law: Catching and Punishing Hackers (cont.):

- 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 or theft a victimless crime?
- Do you think hiring former hackers to enhance security is a good idea or a bad idea? Why?

Identity Theft and Credit Card Fraud

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.

Identity Theft and Credit Card Fraud (cont.)

Stealing Identities (cont.):

- Techniques used to steal personal and financial information:
  - Phishing - e-mail fishing for personal and financial information disguised as legitimate business e-mail;
  - 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 (cont.)

Stealing Identities (cont.):

- Techniques used to protect personal and financial information:
  - 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 (cont.)

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.

Identity Theft and Credit Card Fraud (cont.)

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.

Identity Theft and Credit Card Fraud Discussion Questions

- What steps can you take to protect yourself from identity theft and credit card fraud?
- How can you distinguish between an e-mail that is a phishing attempt and an e-mail from a legitimate business?

Scams and Forgery

- Some scams are similar with pre-Internet period, such as
  - pyramid schemes,
  - chain letters,
  - sales of counterfeit luxury goods,
  - phony business investment opportunities, and so forth.
- If an investment or bargain looks too good to be true, it is probably a scam.
- We examine next three online crime (such as auction fraud, click fraud, and stock fraud), and one offline (digital forgery).

Scams and Forgery (cont)

Auctions:

- Federal Trade Commission (FTC) reports that online auction sites are one of the top sources of fraud complaints:
  - Some sellers do not send items or send inferior products;
  - Shill bidding is used to artificially raise prices;
  - Sellers give themselves or friends glowing reviews to garner consumer trust.
- Auction sites use various techniques to counter dishonest sellers.

Scams and Forgery (cont.)

- Click fraud - repeated clicking on an ad to either increase a site’s revenue or to use up a competitor's advertising budget;
  - Google and Yahoo agreed to pay millions of dollars in disputes with advertisers because of click fraud.
- Stock fraud - most common method is to buy a stock low, send out e-mails urging others to buy, and then sell when the price goes up, usually only for a short time;
  - The Securities and Exchange Commission (SEC) formed an Office of Internet Enforcement to quickly respond to such cases.

Scams and Forgery (cont.)

- The digital technologies allow forgers to quickly and accurately reproduce documents and bills rather than using the old method of printing from engraved plates.
- Digital Forgery - new technologies (scanners and high quality printers) are used to create fake checks, passports, visas, birth certificates, etc., with little skill and investment.
- Defenses:
  - Embedded fibers in paper and special inks that glow under ultraviolet light increase the security of checks, money orders, and identification documents.
  - Some copiers contain a chip that recognizes currency and prevents the copier from making a copy.
  - In the past, banks absorbed the loss from forged checks, but recently the state laws place responsibility on the businesses whose practices made copying checks easy.

Crime Fighting Versus Privacy and Civil Liberties

Search and Seizure of Computers:

- In the context of various computer technologies issues, previous lessons presented tensions between fighting crime, on the one hand, and privacy and civil liberties, on the other.
- Requires a warrant to search and seize a computer:
  - Court rulings were inconclusive about whether information found on computers, but not covered by a warrant, is considered in ‘plain view’.
- Access by law enforcement agents to all the data on a computer can be a serious threat to freedom of speech, privacy, and liberty.

Crime Fighting Versus Privacy and . . . (cont.)

- Automated searches (FTC and SEC):
  - Can monitor constantly and less likely to miss suspicious activity;
  - Can be programmed to only look for what is covered in a warrant.

The Issue of Venue for computer crimes:

- Charges are generally filed where the crime occurs;
- Laws differ between states and countries;
- The location where charges are filed may have a significant impact if community standards apply;
- The FBI usually files in the state where the crime was discovered and the investigation began.

Crime Fighting Versus Privacy and . . . (cont.)

Cybercrime Treaty:

- International agreement to foster international cooperation among law enforcement agencies of different countries in fighting copyright violations, pornography, fraud, hacking and other online fraud;
- Treaty sets common standards or ways to resolve international cases.

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.
  - For example, when the ILOVEYOU virus infected tens of millions of computers worldwide, destroying files, collecting passwords, prosecutors dropped charges against a Philippine man believed to be responsible. The Philippines had no law against releasing a virus at the time. The question is: Should the man be arrested if he travels in the countries affected by the virus?

Whose Laws Rule the Web (Cont.)

Arresting Foreign Visitors:

- A Russian citizen was arrested for violating the Digital Millennium Copyright Act (DMCA) when he visited the U.S. to present a paper at a conference; his software was illegal in the U.S., but not illegal in Russia;
- An executive of a British online gambling site was arrested as he transferred planes in Dallas (online sport betting is not illegal in Britain).

Whose Laws Rule the Web (Cont.)

Libel, Speech and Commercial Law:

- Even if something is illegal in both countries, the exact law and associated penalties may vary;
- 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?

Summary

- Hacking
- Identity Theft and Credit Card Fraud
- Scams and Forgery
- Crime Fighting Versus Privacy and Civil Liberties
- Laws That Rule the Web

Reading suggestions

- From [Baase; 2007]
  - Chapter 5

Coming up next

- The Growing Harm of Not Teaching Malware:
- *Revisiting the need to educate professionals to defend against malware in its various guises.*
- Based on the paper:
  - George Ledin: The Growing Harm of Not Teaching Malware, *Communications of the ACM*, February 2011, vol. 54, no. 2

Thank you for your attention!

Questions?