Crime Cheat Sheet

Description. This handout summarizes principles, laws, frameworks and perspectives that can help in navigating computer crime issues. All of these are discussed in Chapter 5 of the text, which is excerpted and paraphrased below. Use this handout as you consider the crime case studies explored in class, and also as you consider current events.

Hacking (Sec. 5.2.1, pp.254-261)
- The term “hacking” has evolved to mean different things over the years:
  - 1960s-70s: hacking meant writing elegant and clever programs.
  - 1970s-mid-1990s: hacking meant breaking into computer systems, writing and spreading computer viruses.
  - Mid-1990s-now: hacking means gaining unauthorized access to info on the Internet, disrupting the Internet or specific Web sites through various kinds of attacks, and other malicious acts

Political Hacking (a.k.a. “hacktivism”) (Sec. 5.2.2, pp. 263-264)
- Hacktivism is hacking to promote a political cause. Examples include changing a web site in order to protest its message, or launching “denial of service” attacks to disrupt web traffic to a web site to which one objects.
- Some argue that it is ethical: “a modern form of civil disobedience”
- Others argue that, since it causes financial and property damage, it is unethical and should be treated as a crime.

Laws Relevant to Hacking (Sec. 5.2.3, pp. 265-266)
- As a federal law, the Computer Fraud and Abuse Act (CFAA) of 1986 applies to government computers, financial systems, medical systems, and activities involving computers in more than one state (including computers connected to the Internet). Activities it views as illegal include
  - denial-of-service attacks,
  - launching computer viruses or other malicious programs
  - accessing a computer without authorization
  - damaging or destroying information stored on computers without permission
- USA PATRIOT ACT amended the CFAA in the following ways:
  - Expanded the definition of “loss” to allow one to collect damages for costs of responding to a hacking attack
  - Raised the maximum penalty for a first-time offense from 5 to 10 years
  - Increased penalties for hacking into military or criminal justice computers
  - Allowed the government to monitor activities of suspected hackers without court order.
- Several other federal and state laws define crimes related to computer and telecommunications systems, including disclosing passwords, accessing a computer to commit fraud, or interrupting or impairing government operation, public communication, public transportation, or public utilities.

Catching and Penalizing Hackers (Sec. 5.2.3, pp. 266-267)
- Hackers involved in most serious hacking incidents are caught.
- Law enforcement agents are now well tuned in to hacker culture by observing them and through undercover operations.
- “Honey pots”—Web sites that are attractive to hackers—are set up by law enforcement agents to observe hacking behavior
- Hackers are sometimes proud of their exploits and easy to catch; in other cases, large rewards entice people to provide leads
- Computer forensics or digital forensics is the practice of collecting and recovering evidence from computer files. It is a powerful tool in prosecuting hackers.
- Techniques used to catch and prosecute hackers need to be continually updated, because when hackers find out about a particular technique, they can adjust their practices to render the technique ineffective.
• Penalties for hacking depend on the hacker’s intent, age, and the damage done. Difficult cases arise when young people are involved. Should they be given stiff offenses to discourage others? Should they be given jobs in security firms to help prevent others from succeeding? How can we better educate young people so that they use their creative energies elsewhere? According to the author, parents need to take greater responsibility in preventing their kids from engaging in hacking behavior.

Security (Sec. 5.2, pp. 269-273)
• The Internet was originally used primarily for research and communications; there weren’t serious risks, and security measures were either nonexistent or easy to circumvent.
• As the Internet grew, threats became more serious, and security measures have gradually responded in kind.
• Modern security measures include
  o Firewalls, which monitor incoming network traffic and block traffic that is untrusted or suspicious.
  o Requiring the use of “strong” passwords
  o Insurance for hacker attacks
  o Software that detects viruses, phishing attempts, spyware, and the like.
• Responsibility for computer security lies to a great degree with systems administrators (e.g., those of an ISP or WSU information technology staff for WSU networks); however, individuals are also responsible for protecting their own computers, both from attacks from others, and from being taken over and appropriated by others to commit crimes.
• At present, it is not a crime to write computer code that is capable of hacking or spreading viruses; it is protected by the First Amendment. In addition, writing such code is necessary in order to design security responses to it. Should the writing of such code be illegal?

Identity Theft and Credit Card Fraud (Sec. 5.3, pp. 273-281)
• Identity theft is the unauthorized use of someone’s identity in order to purchase items using the person’s credit loans, take out loans in the person’s name, steal the person’s financial assets, and the like.
• There is a large underground market for stolen identities. Complete identities can be purchased for as little as $20. People from 18-29 years of age are the most common victims, perhaps because they most commonly use the web or are least aware of the risks.
• New ways of defending against identity theft are continuously evolving to counter the new ways in which identities are being stolen.
• Common tactics for identity theft:
  o Phishing schemes that request your personal information under false pretenses. The most common scheme, you receive an email that requests you to go to a web site to confirm or update your personal information. The web site is fake and steals the info you enter.
  o Pharming schemes plant false IP addresses in domain name servers (DNS) tables, causing users to unknowingly be directed to fake sites when they type in seemingly valid Web addresses. Once at a fake site, a person’s personal information can be stolen.
  o Spyware is software that one innocently downloads onto one’s computer after connecting to a web site. Spyware tracks keystrokes in order to collect sensitive personal information.
  o Resumes posted online provide a wealth of personal information for identity thieves. More recently, job sites have provided ways to keep sensitive information confidential.
• Measures for protecting against identity theft and reducing damage
  o E-mail programs and web browsers can alert the user if a link is different from the location it claims to be. In addition, some can sniff out sites that are likely to be fake based on poor grammar, geographic location, or other tell-tale signs. Others rate sites based on their trustworthiness; these can prevent access to legitimate sites, however, so one needs to be cautious in using them.
  o Retailers do not store credit card numbers, or store them in encrypted form
  o Financial institutions have added more stringent procedures for authenticating customers; the procedures request personal information beyond one’s account number and password—for example, a favorite number or pet’s name.
Credit card issuers and merchants are willing to absorb some losses in order to provide customers with added convenience (e.g., not having to check IDs, not requiring a signature for small purchases).

If you suspect your identity has been stolen, you can issue a fraud alert, which requires credit bureaus to contact you whenever someone tries to open a new account in your name. It is possible in some states to freeze your credit report, thus preventing creditors from opening new accounts or loans in your name.

**Biometrics (Sec. 5.3.3, pp. 281-282)**

- Biometrics are the unique biological attributes of an individual, including fingerprints, DNA, and eye patterns.
- DNA and fingerprint evidence has been used to solve crimes. These can also be used to help you gain entry to physical structures (e.g., homes, secure areas in airports) or computer systems (especially laptops), and to prevent fraud (e.g., preventing someone from applying for multiple driver licenses under different names).
- While biometrics can improve security, it also has drawbacks. It is just as easy to steal biometric information (stored in computer files) as it is to steal other identifying information. When a person’s biometric information is stolen (e.g., a computer file containing the person’s fingerprint), the person can’t simply get new biometric information.
- Biometric devices can take some measures to prevent them from being tricked. For example, devices that scan irises can flash light to ensure that a real human pupil is being scanned, not a picture. Likewise, devices that scan fingerprints can distinguish real live human tissue from fake tissue.

**Online Fraud (Sec. 5.4 pp. 282-286)**

- Online auction sites like eBay are extremely popular, but also quite susceptible to fraud.
  - Shill bidding is the practice of bidding on one’s own goods to drive up their price. This practice is forbidden in end user agreements, as is the sale of certain items, such as alcohol, firearms, and animals.
  - In a court case involving Bidder’s Edge, a site that uses of automated “bot” software to scrub eBay for products and relist them on their for comparison, a judge ruled that eBay had the right to block Bidder’s Edge’s use of bots, because “eBay's computers are eBay's property” (p. 285).
- Click fraud is the practice of “gaming” online advertising, for which companies are charged a fee based on the number of clicks on it that bring people to their sites.
  - In one form of click fraud, companies repeatedly click on their competitors’ ads, depleting their competitors’ advertising budgets. In another, companies that receive a fee based on the number of times people click on ads repeatedly click on those ads in order to increase their revenues.
  - Click fraud can be reduced by checking and filtering out repeated clicks from the same IP address.
- The Internet can also be used to engage in stock fraud. For example, it can be used to propagate false rumors about a given stock in order to drive its price up. People who engage in such practices have been easily caught. In response, more sophisticated schemes have involving hacking and identify theft have emerged.
- Digital forgery is the use of computing technology to make counterfeit documents, including IDs and money. In addition, photos and videos that are digitally manipulated could be used dishonestly in a court of law. Digital forgery can be addressed through the use of increasingly sophisticated printing techniques and materials, through common sense procedural changes (e.g., a person must send his/her bank a list of the check numbers used), and through new laws that increase the incentive for companies to institute anti-forgery measures.

**Tensions Between Crime Fighting and Privacy/Civil Liberties (Sec. 5.5, pp. 287-299)**

- Fourth Amendment Issues
  - The Fourth Amendment requires that something be in “plain view” of a law enforcement officer in order for it to be admitted as evidence, and that search warrants allow one to search only for specific items. However, when searching computers, a law enforcement officer can see many other files in “plain view.” Can computer files be admitted into a court of law if they are found to be evidence for crimes other than the one for which a law enforcement officer has a search warrant?
  - Can automated surveillance software be legally used by the government to scan the Internet for evidence of fraud, without having a search warrant? Some argue that the use of such software does not require a warrant,
since no human is looking at the data. Others would like private sites to have the right to ban such software from being used, much as eBay was able to ban the use of automated bots by competitors.

- The Sixth Amendment states that a trial must take place near the location of the crime. Where should a defendant in an Internet crime be tried, given that the location may be many different places?

**Difficulties with Enforcing Cybercrime Laws across National Borders (Sec. 5.5.3-Sec. 5.6, pp. 291-299)**

- National laws differ with respect to many items relevant to the Internet, including free speech, intellectual property, hacking/viruses, and gambling.
- A case involving a Russian company that built software that circumvents copyright controls in Adobe’s E-books points out the problem. The software was legal in Russia, but illegal in the U.S. because it violates the Digital Millennium Copyright Act. The Russian author of the software was arrested on a visit to the U.S., but later allowed to return home. The company that produced the software was tried in the U.S. but ultimately acquitted. They agreed to stop distributing their software.
- The Unlawful Internet Gambling Enforcement Act (2006) prohibits credit card and online payment companies from processing transactions involving gambling sites. (Gambling is illegal in the U.S.)
- The so-called cybercrime treaty aims to standardize cybercrime laws across nations. It has weak dual-criminality provisions, which are supposed to dictate that one nation’s government cannot require another nation’s government to cooperate in a criminal justice effort unless the criminal’s act was a crime in both countries. The net effect, according to the author, is that “the cybercrime treaty will likely help law enforcement agencies fight some serious cybercrimes but possibly at the cost of reducing protection for civil liberties in freer countries.”
- Another approach is the “responsibility to prevent access” principle, which states that providers of services and information must ensure that those services and information are inaccessible in places where they are illegal.
- Libel laws differ across countries. If someone writes something that is considered libel in another country but not in his/her own country, where should the person be tried? This situation points out how the “responsibility to prevent access” could be applied: Before publishing something potentially libelous, one should research whether it’s libelous in other countries, and block access to it in those countries where it is libelous.
- An alternative approach is the “authority to prevent entry principle,” which states that a given country can block access to material that is illegal in that country, but may not prosecute the producers of the material so long as the material is legal in the country in which it is produced.