Cybercrime

Defining Cybercrime

- Are crimes involving computers an issue for computer ethics?
- Should there be a separate category for computer crime?
- Try #1
  - Steal a computer
  - Break into a computer lab and snoop
  - Enter a computer lab unauthorized and set a bomb
  - Use a computer to file a fraudulent income tax return
- Try #2
  - A computer is used as a principal tool
  - A computer is a central component
  - Crimes made possible by cybertechnology
- Try #3
  - A criminal act that can be carried out only through cybertechnology and only in the cyberrealm
Three Aspects of Cybercrime

- Cyberpiracy
  - Reproduce proprietary software and information
  - Send proprietary information across a network
- Cybertrespass
  - Gain unauthorized access to a computer system or password-protected website
- Cybervandalism
  - Unleash programs that disrupt transmission of data or destroy system data or other resources

Examples

- ILOVEYOU virus (disruption of network) – vandalism
- denial service attacks on websites – trespass and vandalism
- distribution of proprietary MP3 files – piracy
Hacking

- White hat – nonmalicious
- Black hat – malicious

- Is ”active defense hacking” morally justifiable?
  - Attacks directed against suspected hacker attacks
  - No, can cause harm to the innocent
    denial of service attacks use host computers to launch
Cyberrelated Crimes

- Cyber-exacerbated or cyber-assisted
- Fraudulent income tax – assisted
- Pedophilia, stalking – exacerbated
- Identity theft, corporate espionage
Identity theft

• Using another’s information (name, SSN, CC#’s, etc)) to make purchases or transactions under that person’s identity

• Rise in identity theft via cybertechnology
  – Poor security or carelessness with databases
    * 2005 Bank of America – lost tapes with info on 1.2 million federal employees
    * 2005 Chocie Point and Lexis-Nexis had dossiers on 170,000 Americans illegally accessed ⇒ 750 identity thefts
    * 2005 Laptop with info on 165,000 current and former MCI employees stolen from a parked car
  – Trade in personal information
  – Phishing
  – Spam
Corporate Espionage

- Not all cyberaided, not all directed at tech companies
- Data gathering enhanced by cybertechnology
  - Interception of cell phone conversations
  - Information extracted from websites
- Economic Espionage Act of 1996
  - Federal crime from misappropriation of another’s trade secrets
  - Has cyberspecific language such as ”downloads”
Programs to Combat Cybercrime

- Entrapment and sting operations to catch internet pedophiles
  legal, ethical?
- Keystroke monitoring
- Carnivore – packet sniffer
- TIA – terrorist information awareness uses data mining
- Patriot Act and enhanced government surveillance techniques
Jurisdiction in Cyberspace

- Example: virtual casino
- Legal jurisdictions are based on physical spatial boundaries that are absent in cyberspace
- Cybercrimes often cross jurisdictional boundaries
- Is cyberspace a place, a public space, or a broadcast medium like TV or radio?
Legislation

• Patriot Act allows "sneak and peek" attacks on individuals and organizations suspected of criminal acts

• Magic Lantern
  – Trojan horse that uses keystroke monitoring to obtain encryption keys
  – Needs cooperation of software vendors
  – Can leave security holes (back door or trap door) to be exploited by others

• US Legislation covers fraud involving computers, communication systems, unlawful access to communications, requirements for government access

• International Code (Council of Europe, 2000) covers confidentiality, availability and integrity of data and computer systems, computer related offenses such as fraud, content related offenses such as child porn, copyright offenses
Tools and Techniques to Combat Cybercrime

- Encryption
  - Strong encryption supports criminal acts
  - Clipper Chip
    * encryption system
    * installed on all electronic communication devices
    * keys held by a government agency, released on court order
    * no independent testing
    * no safeguards against abuse
    * loss of international sales
    * threat to civil liberty (4th amendment, search and seizure)
• Biometric Technology

- biological identification of a person
  eyes, voice, retina, handwriting, finger or hand prints
- 2002 used iris scan at Heathrow airport for ID
- Eurodac – biometrics used to control illegal immigration in EU
  subject to debate, like Clipper chip
- Human rights violation?
  * error – criteria for a match are variable
  * abuse – original use could be expanded
  * privacy – benefits may not offset loss of privacy