Lecture notes for 11.5 Computer Crime

Computer crime
- Def: Any activity where a computer or network is the source, target, or place of a crime
- Unauthorized access, interception, or interference
- Misuse of devices, forgery, fraud

Examples of computer crime
- Espionage
- Corporate espionage
- Botnets: DoS used for extortion
- Black economies: credit card dumps
- Warez (copyrighted works traded in violation of copyright law)
- Hacking (acquiring unauthorized access)
- Child pornography distribution
- Website defacement
- Stalking / harassment
- Identity theft
- Telecommunications theft
- Hate speech (Nazism prohibited in Germany... international effects?)
- Drug trafficking
- Terrorism

Laws
- Legal system moves much more slowly than computer world
- Most US laws are 1996 or later
- Computer Fraud & Abuse Act, CAN-SPAM, DMCA, Electronic Communications Privacy Act

Crypto
- US export control prior to 1998 (largely ineffective)
- Key escrow (public resistance)

Investigating agencies (in US)
- FBI
  - Computer intrusions & malware spread
  - Online crimes against children
  - Intellectual property violations
  - National & transnational organized crime engaged in Internet fraud

- Secret Service
  - Fraud concerning “federal interest computers”
  - Computers used in counterfeiting & false ID creation
  - Financial crimes: bank account hacking, cell cloning, counterfeiting of corporate checks

Crime [complexities in the computer world]
- Who is the wronged party?
- Who is the responsible party?
- What is the financial loss?
  - What is the value of data?
- Do law enforcement officers, lawyers, jurors, judges, legislators understand the area?
- Do we understand the area? When does an attack become a crime?

Endpoint
- Network monitoring may reveal illegal computer use
- Does not reveal user
- Challenge: connect illegal use to user
  - “A virus did it” has been an attempted defense
  - Suspect was a *stepping stone*
- If an attacker breaks uses your system as a stepping stone because you didn't patch, should you be responsible?

International matters
- Computer crime trivially crosses international borders, no physical proximity between attacker & victim
- Consider action undertaken by A against B
  - In A's country, the action was not illegal (and might have been encouraged)
  - In B's country, the action was illegal
  - Has a crime occurred? Has A committed a crime?
- Consider communication between A and B
  - In A's country, the contents of the communication are legal
  - In B's country, the contents of the communication are legal
  - The transmission crosses country C, where the contents are illegal
  - Have A and B committed a crime?
  - Has the ISP in country C committed a crime?