Ethical, legal, and policy issues related to security and privacy research and practice
Things to consider

- Criminal law
- Civil law
- University policy
- Community standards for ethics
Criminal and civil law
Access Device Statute

• Access device
  – Any card, plate, code, account number, electronic serial number, ... that can be used to obtain money, goods, services, or anything of value ...

• Unauthorized access is criminal whether or not a computer is involved
Computer Fraud and Abuse Act

- Acts that compromise computer network security
- Protected computer means:
  - Used by the U.S. government, or...
  - Used by financial institutions, or...
  - “used in interstate or foreign commerce or communications”
- *I.e.*, nearly all networks
- Unauthorized access by outsiders or exceeding authorized access to commit crimes
- State alternatives
Electronic Communications Privacy Act

- Two parts
  - One amended the Wiretap Act (1918)
  - Other amended the Stored Communications Act

- Wiretap act
  - Protects wire, oral, or electronic communication in transit against interception in an illegal manner

- Exceptions for the government
Cyber Security Enhancement Act of 2002

- Bodily harm or possible death, public safety
  - Could face life in prison
Digital Millennium Copyright Act (DMCA)

• Passed in 1998

• “Civil and criminal liability for the use, manufacture, and trafficking of devices that circumvent technological measures controlling access to, or protection of, the rights associated with copyrighted works” [GHH 4th edition]

• Exemptions for encryption research and security testing
  – Other exemptions 3 years at a time

• Universities risk losing federal funding
DMCA, EFF's list of legally risky activities...

- EULAs, TOUs, NDAs, etc.
- Software you do not possess legally, or unauthorized copies
- "Technical protection measures", e.g., authentication handshakes, protocol encryption, password authentication, code obfuscation, code signing
- Copying code
- Network packet inspection
Limiting legal risk (from EFF)...

- Consult a lawyer
- Watch out for “no reverse engineering” clauses
- Watch out for “technical protection measures”
- Careful dissemination of results
  - *E.g.*, don't include copied code
Ethical Disclosure

• Different points of view
• CERT/CC is a good choice if you’re not sure
• 45 days from reporting to publishing is the “CYA” minimum
University policy
UNM Policies

• 2500: Acceptable Computer Use
  – Many considerations, including FERPA and PCI
  – They can log into your account
• 2520: Computer Security Controls and Access to Sensitive and Protected Information
  – Don’t run Wireshark on others' network traffic unless you're a department head or designee (probably not even then)
• 2550: Information Security
  – “higher education institutions are considered financial institutions”
• Also consider:
  – FOIA and the New Mexico Sunshine Act
• Things I’ve been told
  – Don’t run nmap on University computers, except on the research network
  – Don’t run wireshark on University networks (closed research networks are okay)
  – Running Tor is okay, even Tor relays, but not Tor exit nodes
Community standards for ethics
Research ethics

• Belmont and Menlo reports
  – Information about individuals, or...
  – Interventions in their environment

• Examples for discussion
  – Users around the world given software to test Internet censorship
  – Spoofing IP return addresses

• IRB process
  – You can get a “Does Not Apply” Letter in cases where IRB approval is not required but program committees might feel otherwise
Ethical Hacking Process

• Penetration testing
  – Get everything in writing
  – Establish ground rules
  – See Gray Hat Hacking 4th edition for more info

• Authorized access is always okay
  – If I tell you to, e.g., get root on a VM as part of an assignment, I have authorized you to do so
Sources

- Gray Hat Hacking, Fourth Edition by Regalado et al.
- https://www.eff.org/issues/coders/reverse-engineering-faq
- http://policy.unm.edu/