Legal and Ethical Issues Facing Cybersecurity Researchers
Aaron Burstein
UC Berkeley School of Law

The Problem

• A complex and sometimes unclear body of U.S. law constrains cybersecurity research activities:
  – Communications privacy
  – Copyright
  – Contracts
  – Computer fraud & abuse
• Ethical obligations may impose further constraints.
Overview

• Three case studies
  – Collecting and sharing network packet traces
  – Analyzing software
  – Running infected hosts
• Identify and explain legal issues in each case
• Identify individual, institutional interests that influence ethical considerations

DISCLAIMER

These materials provide a general discussion of legal issues facing cybersecurity research. This discussion is not intended to provide individualized legal advice.
Definitions

• “Laws” include statutes, regulations, court decisions.
• “Ethics” is concerned with what one should or should not do, regardless of whether it is legally permissible.
  – Understanding the interests protected by law and organizational (i.e., a researcher’s university or employer) interests can help guide ethical decisions.

Example 1: Obtaining Data from Networks

• Two separate concerns:
  – Collecting network measurement data (e.g., packet traces)
  – Publishing data
• Legal issues
  – Communications privacy laws
• Ethical issues
  – Respecting users’ privacy
  – Respectful uses of published traces
Electronic Communications Privacy Act (ECPA)

  - Prohibits real-time interception of communications contents
- Stored Communications Act (18 U.S.C. § 2701-110) ("SCA")
  - Prohibits certain disclosures of content and noncontent/addressing information
- Pen Register/Trap and Trace statute (18 U.S.C. § 3121-27) ("Pen/Trap")
  - Prohibits real-time interception of noncontent/addressing information

No Research Exceptions in ECPA!

- Some trace collection permitted by:
  - Consent of users or
  - "Provider" exception (allowing network operators to monitor networks to defend them)
- Limitations
  - Individual consent hard to get
  - Blanket consent (e.g., as part of a network’s terms of service) may provide little information about data collection, use
  - Provider exception requires collaboration with operational IT staff
How ECPA Affects Cybersecurity Research (1)

• Activity: Collecting full-packet traces in real-time
  – Relevant law: Wiretap Act
  – Applies to any network (government, enterprise, WiFi, university, etc.)
  – Need consent or sufficient link to operational network protection for provider exception
  – Wiretap Act continues to cover traces after they are recorded \If collection violates law, disclosure probably does too.

How ECPA Affects Cybersecurity Research (2)

• Activity: Collecting packet-header traces in real-time
  – Relevant law: Pen/Trap statute
  – Consent, provider exceptions available
  – Also an exception for network “operation, maintenance, and testing”
  – Legally stored data become subject to SCA
How ECPA Affects Cybersecurity Research (3)

• Activity: Sharing or publishing packet traces
  – Relevant law: SCA
    • Applies only to “public” service providers: commercial ISPs but not businesses
  – Full-packet traces: disclosure prohibited without consent, subpoena
  – Packet header traces: disclosure allowed unless given to “governmental entity”
    • Much broader than law enforcement; hampers some public releases

Ethical Dimensions of Trace Collection and Analysis

• ECPA extends 4th Amendment right protecting individuals against unreasonable government searches to non-government actors.
  – Communications records can reveal a huge amount of information about individuals.
• Many users expectations’ of privacy protection from network providers sometimes outstrip legal protections.
Impact of Communications
Privacy Ethical Considerations

• Data collection/sharing plans should go beyond legal issues to consider:
  – De-identifying data (and possibilities of re-identifying it) to protect individuals;
  – Costs, benefits of limited disclosure versus unrestricted publication;
  – How to enforce limited disclosure agreements; and
  – Effects on the researcher’s organization (e.g., compliance with privacy policies)

• Summary: It is essential to vet plans with IT and legal officials from the host organization.

Example 2: Security Analysis of Software
Software Analysis: Legal Issues

• Issues
  – Finding software vulnerabilities
  – Publishing results

• Relevant laws:
  – Contract law (EULAs, clickwrap/shrinkwrap licenses)
  – Digital Millennium Copyright Act (DMCA)

Software Analysis: Contract Issues

• EULAs typically prohibit reverse engineering, other processes that reveal vulnerabilities
• Courts usually enforce them . . .
• . . . but important issues remain unsettled:
  – Pre-emption by patent law
  – Tension with First Amendment
Software Analysis: DMCA Issues

• “No person shall circumvent a technological measure that effectively controls access to a work protected” by the Copyright Act
• But: courts, U.S. DOJ have found that the DMCA does not prohibit conducting research on or publishing papers about software vulnerabilities.
• Caveats:
  – Publishing actual circumvention software might violate DMCA.
  – Restrictions in EULAs still apply.

Ethical Issues in Software Analysis

• Whether (and when) to notify software vendor
• How much detail to publish
Example 3:
Running Infected Hosts

Running Infected Hosts: Legal Issues

• Contexts
  – Running malicious code in testbeds
  – Running honeynets to interact with attackers

• Legal Issues
  – Computer Fraud and Abuse Act (CFAA)
  – Child pornography possession
Testbeds: Legal Issues

• Concern: What if worms, viruses escape testbed containment?
• CFAA (18 U.S.C. § 1030) prohibits *knowingly* obtaining unauthorized access to an Internet-connected computer
  – Unclear whether accidents involving testbeds meet this standard of intent

Honeynets: Legal Issues

1. Remote attackers use honeynet hosts in attacks.
   • CFAA is a concern:
     • “Ostrich” defense (willful ignorance) doesn’t work
2. Attackers plant contraband data, e.g., child pornography.
   • Mere possession raises serious legal issues; contact institution and legal counsel immediately
3. Research hosts, subnets might avoid ECPA issues because there are no actual users.
Honeynets: Ethical Issues

• Host organization reputation
  – Could honeynet activity look like bad network management to others?
• Can attackers learn from you (and how much)?

SCA: Content

• “[A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” (18 USC § 2702(a)(1))
• Exceptions: compulsory process, consent, provider protection
“Electronic Communication”

• “[E]lectronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce” (with some exceptions) (18 USC § 2510(12))

SCA: Noncontent Disclosure

• “[A] provider of . . . electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity.”
• Exceptions: Compulsory process, consent, provider protection, non-governmental recipient.
Resources

• Legal Information Institute (http://www.law.cornell.edu/)

• Samuelson Clinic at UC Berkeley School of Law (http://www.samulesonclinic.org/)

• Toward a Culture of Cybersecurity Research (http://ssrn.com/abstract=1113014)
  – In-depth analysis of applicable privacy laws and proposal for a research exception to the ECPA