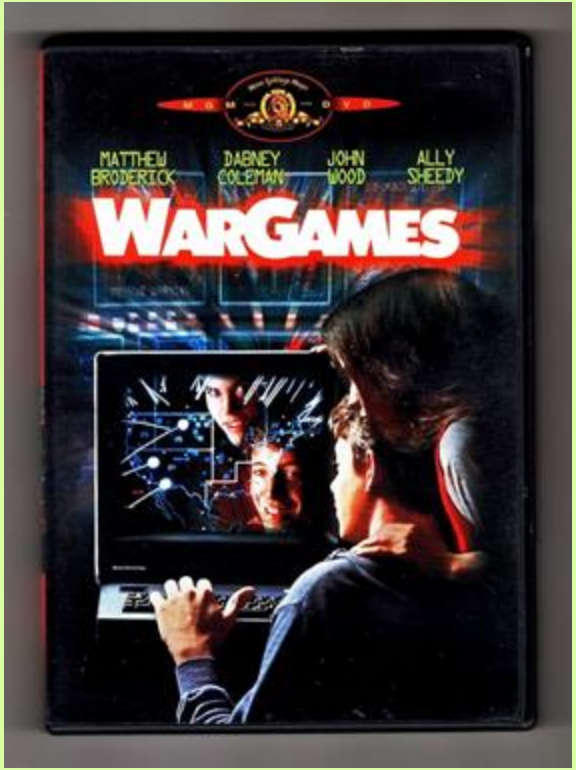
Vulnerability Disclosure + Research Law

Shiri Huber and Gordon Chan, BU School of Law

April 02, 2025

1. Intro to the law + its application to hardware
2. Norms of disclosing research to companies
3. First Amendment protections

Agenda


MATTHEW BRODERICK
DABNEY COLEMAN
JOHN WOOD
ALLY SHEEDY
WARGAMES


MGM

Computer Fraud and Abuse Act (CFAA)

- Federal anti-hacking statute
- Creates **civil** + **criminal** liability
- Culpable conduct:
  - **Intentionally** access **a computer**
  - **Without authorization** OR exceeding authorized access
  - And thereby **obtaining information**
  - From almost any computer

- Conduct research on a device you do not own and do not have permission to access

Could be liable

- Accessing your own device
- Accessing a device you DO NOT own BUT have permission to access
- Accessing a device you do not own BUT all the resources you access are (1) publicly available OR (2) you have valid credentials issued to you that provide access to them

Not liable

Think of your own research/work/experiences -- does any of it bring up the conduct implicated in the CFAA?

DMCA §1201

- Creates liability for bypassing or removing controls/access mechanisms on copyrighted works

- Creates **civil** + **criminal** liability

- Culpable conduct:
  - Descramble, decrypt, avoid, bypass, etc.,
  - A technological measure [a process/information that controls access to the work w/copyright owner's permission]

- Underlying work is copyrighted AND you circumvent controls
- Examples:
  - CAPTCHAs
  - Digital Rights Management schemes (DVDs, video games)
  - Code signing
  - Encryption

Could be liable

- Underlying work NOT copyrighted
- Unauthorized use of username and password (maybe)
- Purely physical protections
- **Security/encryption testing** with authorization
- **Good-faith security research**

Not liable

Beware! Software Licenses + Other Contracts

- End User License Agreements = detail how someone should use software
- Terms of Service/Terms of Use = comes with websites, apps, devices, etc.
- NDAs = non-disclosure agreements

Beware also!

- State laws -- many have their own version of the CFAA
- Export control laws

Discuss:

1. Turn to the person next to you

1. Now that you have a better understanding -- revisit your own research or work, how does the law apply?

1. Share with the class

Beyond the Statutes
Legal Risks and Norms

Overview

- Understanding Different Legal & Ethical Frameworks
- Different Consequences of Hardware & Software Vulnerabilities
- Vulnerability Disclosure and Unique Legal & Ethical Challenges

Norms & Practices:

Coordinated Vulnerability Disclosure (CVD)

What is it?

- Process of how to privately inform about security flaws prior to public disclosure

Key Features

- Disclosure window (90 - 180+ days)
- Contact via secure means
- Deliberation on patch readiness
- Publication of CVE & technical paper

Companies Support CVD & Other

- Public platforms
- Trusted intermediaries
- Other: Hardware Bug Bounty programs

Challenges

Long Patch Cycles

- Vulnerability persistence
- Logistical restrictions
- Examples:
  Specter and Meltdown

Lack of Pathways

- Lack of channels
- Unknown contacts
- Company ignorance

IP Restrictions

- Trade secret protection
- IP or EULA violations

Supply Chain Issues

- Downstream impacts
- Difficulty in coordination

Legal Ambiguity

- Unclear liabilities
- No guaranteed safe harbor
- Threats of legal action

Challenges

Long Patch Cycles

- Vulnerability persistence
- Logistical restrictions
- Examples:
  Specter and Meltdown

Lack of Pathways

- Lack of channels
- Unknown contacts
- Company ignorance

IP Restrictions

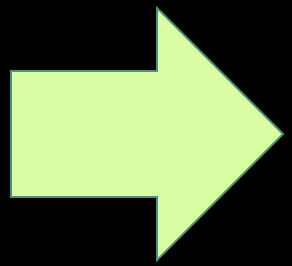
- Trade secret protection
- IP or EULA violations

Supply Chain Issues

- Downstream impacts
- Difficulty in coordination

Legal Ambiguity

- Unclear liabilities
- No guaranteed safe harbor
- Threats of legal action



Are ya scared? No worries! SILC is here to save the day

Pros

Cons

Examples

Ethical Considerations?

Pros

- Promotes transparency
- Prevents delays
- Educates community

Cons

- Exploitation
- Broad repercussions
- Downstream impacts

Examples

- St. Jude v. MedSec & Muddy Waters

Ethical Considerations?

First Amendment

Code as Speech

Key Cases

- Bernstein v. U.S. D.O.J. (1999)
- Junger v. Daley (2000)

Speech vs. Conduct

- Legal distinction between speaking vs. doing
  - Publishing vs. conducting
  - BUT ⇒ intent

Potential 1st Amend. Issues

Conflicts with DMCA

- No definitive rulings
- Green v. D.O.J. (2020)

Export Control Laws & 1st Amendment

- "Born classified" doctrine

NDAs, Private Restraints, Contracts

- NDAs, licensing agreements, EULAs
  - Breach of contract
  - Reverse engineering clauses

Prior Restraints & Injunctions

- Government & "prior restraint"
- BUT ⇒ injunctions & private action
  - MBTA v. Anderson

Key Takeaways

Publishing Isn't Always Safe

Know Legal Boundaries

Coordinate Disclosure

Advocate!

Thank you & questions