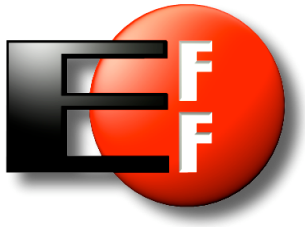

I Voted? How the Law Increasingly Restricts Independent Security Research

Cindy Cohn
EFF Legal Director
<http://www.eff.org>

The Electronic Frontier Foundation

Why do we need independent security research?

- Why not *caveat emptor*?
  - Vendors are not always motivated
  - Customers are not always capable
  - Sometimes researchers are customers
- Good security is in the public interest
  - Insecure private systems affect others
    - Internet worms
    - Zombies
  - Insecure public systems affect us all

The Electronic Frontier Foundation

An insecure public system

DIEBOLD ELECTION SYSTEMS

```
#define DESKEY
((des_key*)"F2654hD4")
```

```
/* This is a bit of a
   hack for now [...] */
```

The Electronic Frontier Foundation

An insecure public system

DIEBOLD ELECTION SYSTEMS

- Diebold AccuVote election system code leaked
  - (They left it lying around on a public FTP server)
- E-voting activists downloaded the code and distributed it far and wide

The Electronic Frontier Foundation

An insecure public system

DIEBOLD ELECTION SYSTEMS

- Rubin, Wallach et al. did an independent assessment of Diebold's code
- They found:
  - Serious implementation flaws
  - Bad crypto
  - An attack allowing one person to vote multiple times

The Electronic Frontier Foundation

An insecure public system

- Results from the study: real electoral reform
  - Heightened awareness of voting security issues
  - Diebold AccuVote system decertified in California
  - Paper trail requirement passed in many states; pending in Congress
  - Spurred state-sponsored reviews like the recent “top to bottom” review in California

The Electronic Frontier Foundation

Voting security, meet the law

- The Diebold report authors had to navigate several legal issues before they could publish
- EFF assisted from the very early stages of the research
- Today:
  - How the law could have impeded the Diebold report
  - How the law can affect your research

The Electronic Frontier Foundation

Some laws that affect independent security research

- Classical copyright law
- Digital Millennium Copyright Act (DMCA)
- Computer Fraud and Abuse Act
- Trade secret law

The Electronic Frontier Foundation

Copyright law

- Grants authors exclusive rights in their work
  - "to reproduce the copyrighted work"
  - "to prepare derivative works"
- Anything you write down is copyrighted
  - "fixed in any tangible medium of expression"
  - Registration is not required
  - Unpublished, secret work is fully protected

The Electronic Frontier Foundation

Copyright law

- Diebold owns the copyright in its e-voting code
- In order to study the code, researchers had to make copies
  - If they had chosen to run the code, they would have made additional copies (in their computers' RAM)
  - RAM copies have been held to infringe
- Copyright law provides for damages of up to $150,000 per infringement

The Electronic Frontier Foundation

Copyright law

- Fortunately, copyright is not an absolute right
- Fair use is a defense to infringement
- A balancing test involving several "factors":
  1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;
  2) the nature of the copyrighted work;
  3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and
  4) the effect of the use upon the potential market for or value of the copyrighted work.

The Electronic Frontier Foundation

Copyright law

- Translation: You get to pay a lawyer to argue that your fair use counterbalances their copyright
  - There are no cut-and-dried legal standards defining fair use
  - You're welcome to make copies if you can later show in a court of law, after extensive litigation, involving discovery of nearly everything related to your research, with tens or hundreds of thousands of dollars of damages to your institution at stake if you lose, that what you did was fair use.
- Feel better now?

The Electronic Frontier Foundation

Digital Millennium Copyright Act

- "No person shall circumvent a technological measure that effectively controls access to a [copyrighted] work"
- Some of the leaked Diebold files were (trivially) encrypted ZIP archives
  - Decrypting these archives might violate DMCA
  - There is no fair use defense to circumvention
  - Diebold report authors, advised by EFF, decided not to decrypt the ZIP files

The Electronic Frontier Foundation

Digital Millennium Copyright Act

- Result: Less of the Diebold code was reviewed than the researchers wanted
- What if all of the code had been trivially encrypted?
  - We might not have gotten good research into Diebold voting machine flaws at all
  - A less obvious way that the DMCA prevents research

The Electronic Frontier Foundation

Digital Millennium Copyright Act

- It is illegal to make or distribute code that:
  - "is primarily designed or produced for the purpose of circumventing a technological measure that effectively **controls access** to a [copyrighted] work"
  - "is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively **protects a right of a copyright owner** under this title in a work or a portion thereof"

The Electronic Frontier Foundation

Digital Millennium Copyright Act

- What kind of code is illegal?
  - DeCSS (DVD decryption)
  - Source code that shows how to bypass some DRM
  - A high-level description of such code?
  - An academic paper?
- Hyperlinks to circumventing code ruled illegal in narrow circumstances

The Electronic Frontier Foundation

Digital Millennium Copyright Act

- SDMI Challenge
- Group led by Ed Felten found serious problems with the recording industry's content protection tech and wanted to present it at an academic conference
- For their trouble, they got threatening letters from RIAA lawyers and many, many conference calls with lawyers
- Helped by EFF, they brought the matter to court. RIAA backed down.

The Electronic Frontier Foundation

Computer Fraud and Abuse Act

- The federal computer intrusion law
  - Illegal to access a protected computer without authorization (protected computer = Internet)
  - Civil and criminal penalties for violation
- What if Diebold had claimed that an intruder stole their election code?
  - Researchers might have to show in court that they didn't misappropriate the code

The Electronic Frontier Foundation

Computer Fraud and Abuse Act

- There's a larger point here, too
- Why is it necessary that code being researched has to just drop out of the sky?
  - Researchers were able to do the Diebold research because someone accessed a Diebold server
  - CFAA gray area
  - Should law-abiding researchers have to depend on people willing to risk violating the law?

The Electronic Frontier Foundation

Trade secrecy law

- State law, different in every jurisdiction
- California: information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

  (1) Derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and

  (2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.
- Civil and criminal penalties for:
  - Directly misappropriating trade secrets
  - Disseminating information you "know or should have known" is a wrongfully acquired trade secret

The Electronic Frontier Foundation

Trade secrecy law

- Was the Diebold code a trade secret once it leaked onto the Net?
  - At first, probably yes, but by the time the researchers started work, 6 months later, probably not in California: *Bunner* DeCSS case
  - But had to look to all possible states: California, Maryland, Texas and Ohio
- If it was, researchers might be liable
  - For distributing the code among their team
  - Or for discussing aspects of the code Diebold would prefer to keep secret

The Electronic Frontier Foundation

Trade secrecy law

- Many vendors would love to claim that their security flaws are trade secrets
- Reverse engineering is a defense
  - But not all security flaws can be found by reverse engineering
  - Plus you might not be allowed to reverse engineer
    - Have you read your EULAs lately?
- Institutionalizing security through obscurity

The Electronic Frontier Foundation

Conclusion

- Independent security research is crucial
- But it's not without legal pitfalls
- Vendors are often unhappy when someone points out the flaws in their products
  - Their first reaction is often to call their lawyers
- EFF is committed to ensuring that researchers can study and publish their work freely

Q & A

The Electronic Frontier Foundation

Acknowledgments

- EFF clients and heroes: Dan Wallach (2x), Adam Stubblefield (2x), Avi Rubin, Tadayoshi Kohno, Ed Felten, Bede Liu, Scott Craver, Min Wu, Ben Swartzlander, Drew Dean, Usenix Association, and many others who we cannot name in order to protect the attorney/client privilege.
- EFF Intern: David Price