DMCA and the Effects of Regulating Computer Security Research and Discussion

Edward W. Felten
Department of Computer Science
Princeton University
felten@cs.princeton.edu

[currently on sabbatical at Stanford Law School]

Importance of Infosec

- Information security is vital for nation, and for citizens
- Problem requires public/private cooperation
- Our nation is the most vulnerable, and the best able to address the problem
- Challenges include education, operations, and R&D

Infosec Research

- Computer security research has two prongs:
  - Synthesis: design new systems
  - Analysis: find strengths/weaknesses of existing systems
- Synthesis and analysis go hand in hand
- Experience teaches the value of analysis
  - Find problems before system is deployed
  - Learn what to do differently next time
  - Develop sense for where problems really come from
  - Teach next generation of designers by example

Analysis, Markets and Policy

- Analysis benefits consumers
  - Learn about current risks, how to mitigate them
  - Evaluate long-term risk levels and trends
  - See track records of companies, methods
  - Compare marketing to reality
- Analysis benefits policy makers, for roughly the same reasons

AES: A Success Story

- Advanced Encryption Standard (AES) illustrates success of open analysis.
- AES process brings private analysts on board, factors in their results.
  - Encourage analysis and discussion
  - Break systems before deployment
- Result is widespread trust in the process, buy-in to the resulting standard

DMCA: Regulating Analysis

- Recent trend toward regulating security analysis and discussion of analysis
- Digital Millennium Copyright Act (DMCA), Section 1201
  - Outlaws circumvention of technology that mediates access to copyrighted material
  - Outlaws trafficking in "technologies" that are "primarily designed or produced for the purpose of circumventing" such technology
  - Limited exceptions, not of much help in practice

DMCA Rationale

- Concern about copyright infringement
- Build DRM (copy protection) technologies
- But DRM never seems to work
- So outlaw DRM-breaking technologies, discussion of weaknesses in DRM systems

- Proponents claim no impact on legitimate security work
  - but security researchers alarmed by passage of DMCA

DMCA, Three Years Later

- DMCA used to muzzle security researchers
  - Felten team's research on watermarking
  - Ferguson analysis of digital TV crypto
  - Analysis of Microsoft's DRM
- DMCA *not* used against infringers
- Courts rule that
  - DMCA violation can occur without infringement
  - Tool can violate DMCA even if it cannot possibly be used to infringe

My Story

- Industry consortium (SDMI) considering four technologies for deployment in next-gen music and players.
- We (Princeton, Rice, Xerox researchers) study technologies, find that they don't work very well.
- We write a paper detailing our findings.
- Paper accepted for publication at conference.

Our Paper

- Music industry claims that our paper is a "technology" whose primary purpose is copyright circumvention
  - Similar claim for oral presentation
- Threatens to sue authors of paper, conference organizers, and employers
- Seeks control over contents of paper

Watermarks for Music Security

- Industry goal: prevent playing and/or copying of music files (without their permission)
  - Prevent copyright infringement
  - Prevent some fair use as well
- Watermarking: add faint noise to file, to mark file as copyrighted, and to state restrictions on use
  - Watermark is supposed to be inaudible, non-removable, tamper-evident

SDMI-Style Watermarking

- Before releasing music
  - Add watermark to music
- In every music player/recorder:
  - Check song for watermark
  - If no watermark: allow any use
  - If watermark is present: read instruction bits from watermark, obey them
    - Refuse to do anything if tampering detected

Do Watermarks Work?

- Goals of attacker
  - Remove watermark, or render it undetectable
  - Modify bits stored in watermark
- Attack methods
  - Blind signal-processing attacks
  - Determine how watermark works, experimentally
    - Known plaintext attack, or without plaintext
  - Reverse-engineer detector in player
  - Build your own noncompliant player/recorder, or modify existing one to make it noncompliant
- Not clear that watermarking can work!

Our Study of SDMI Watermarks

- Different types of watermarks
  - Echo hiding
  - Boost certain frequencies selectively
  - Phase distortion
- All can be defeated if you know how they work, and often if you don't
  - Requires moderate effort, moderately skill

Why This Isn't Surprising

- Kerckhoffs's Principle: Security of a system shouldn't rely on keeping the security algorithm secret
  - Instead, rely on keeping a numeric key secret
- SDMI-style watermarking must violate this principle, since music player must detect watermark "blindly"

Non-watermark Attacks

- Watermarking does not provide end-to-end (musician to listener) protection
  - Attacker grabs content after watermark processing has occurred
  - No obvious solution to this problem
- Unauthorized copying will still be possible, for serious pirates

If you can listen to it, you can record it.

My Story (cont.)

- Music industry (RIAA, SDMI, Verance) threatens lawsuit if we publish.
  - Conference organizers also threatened. We withdraw paper because of threats.
- We file lawsuit seeking right to publish.
- After legal wrangling, paper is published.
- We managed to publish, but:
  - Months of effort by researchers lost
  - Hundreds of lawyer-hours spent ($$$)
  - Member of our team loses his job
  - Eight-month delay in release of our results

DMCA as a Ban on Analysis

- Common DMCA scenario: advocates of a broken technology try to prevent customers from finding out that it is broken.
- DMCA makes it risky to analyze any technology that is used by somebody, somewhere to mediate access to copyrighted material.
- Apparently outlaws even discussion of flaws in such technologies.

Is the DMCA Working?

- Advocates cite DVD as success story
- But
  - DVD crypto laughably weak, easily broken
    - Industry must have known this would happen
  - DMCA failed to prevent creation, distribution of circumvention tools
  - DVDs a big success in the market anyway

Next Step: Mandating DRM

- Industry now says DMCA isn't enough; seeks laws requiring that all digital devices include specific DRM technologies.
  - "Approved" list includes some technologies that have already been broken.
  - But: high barriers to acceptance of new technologies onto list.
  - Proposed mandates *require* that implementations be hard to analyze.

Pro-Innovation Policy

- Foster development of new technologies
- Foster analysis, especially before deployment
- Foster adoption of proven methods

- Open process allows debate, education.

DMCA and the Effects of Regulating Computer Security Research and Discussion

Edward W. Felten
Department of Computer Science
Princeton University
felten@cs.princeton.edu

[currently on sabbatical at Stanford Law School]