The Law of ‘Sploits

Jennifer Stisa Granick, Esq.
Stanford Law School
Center for Internet & Society
jennifer@law.stanford.edu
650-724-0014
Security Publication: Pros

• Public Awareness of Security Risks
• Enables SysOp Remediation
• Motivation for Vendor to Patch
• Consumer Rights
• White Hats Know What Black Hats Know: No Security Through Obscurity
Security Publication: Cons

• Public Relations Nightmare: Relative Seriousness of Problem
• Window of Opportunity Before Patch
• Script Kiddies: Greatly Increases Potential Attackers
Security Publication

Dual Nature:
The same information that allows more widespread exploitation of vulnerabilities is required to correct those vulnerabilities.
Security Publication: Issues

• Security Through Obscurity vs. Script Kiddies
• Full Disclosure vs. Limited Disclosure
• Exploit/Proof of Concept Code
Legal Liability?

• Negligence: Duty Not to Publish?
• Conspiracy: Agreement?
• Wire Fraud: Intent to Defraud?
• State Statutes?
• Digital Millenium Copyright Act
• Council of Europe Convention on CyberCrime
DMCA: International Law

- WIPO Treaty
- International Versions
DMCA

• Prohibits Circumvention of Technological Measure that Effectively Controls Access to a Copyrighted Work

• Prohibits Manufacturing and Distribution of Any Technology (Tools)
  – Primarily Designed for the Purpose of Circumventing Access Controls
  – Limited Commercially Significant Purpose
  – Marketed for Use in Circumvention
DMCA: Exceptions

• Security Testing
• Encryption Research
• Reverse Engineering
Security Testing Exception

- information derived used solely to promote the security of the owner or operator of the tested computer system, or
- information obtained shared directly with the developer of the system
- information obtained distributed in a way that might enable copyright infringement or other legal violations
Encryption Research Exception

• Professional Cryptographers
• Seek Advance Permission
• Necessary to Advance the State of the Art
• Publishing Results Does Not Promote Infringement
Reverse Engineering Exception

- Purpose to Achieve Program-to-program Interoperability
- Reverse Engineering Is Necessary
- Information Divulged for the Sole Purposes of Enabling Program-to-Program Interoperability
COE CyberCrime Treaty

- 32 signatories, including US
- Article 6: Illegal Devices: Prohibits computer programs designed or adapted primarily for the purpose of gaining unauthorized access to computers, intercepting data or interfering computer systems.
- Signatories may allow devices if not for the purpose of committing an offense.
First Amendment

• Source Code is Speech:
  – Karn v. Department of State: Source Code
  – Bernstein v. Department of Justice

• Binary Code:
  – Universal City Studios v. Reimerdes/Corley
  – DVD CCA v. Bunner
  – US v. Elcom Ltd.
1st Am. Limits Regulations?

- Program is both Communicative and Functional
- Communication can be regulated if sufficiently important government interest in regulating the non-communicative or functional aspects
• Other Countries?
• More Harm Than Good from Banning Security Publications?
• Convince Publishers to Release Information in a Manner than Maximizes the Pros and Minimizes the Cons
• Enforcement Mechanism?
• Who Bears the Costs When the System Doesn’t Work?
CyberSecurity Research & Disclosure

• Conference at Stanford Law School
• November 2003
• More Info:
  http://cyberlaw.stanford.edu/security/