Outline

1 Research
   - Introduction
   - Model
   - Researchers
   - Summary

2 Survey
   - Introduction
   - Brungs-Jamieson Survey
   - Liles Survey
Outline

1 Research
   - Introduction
   - Model
   - Researchers
   - Summary

2 Survey
   - Introduction
   - Brungs-Jamieson Survey
   - Liles Survey
Toward a Culture of Cybersecurity Research

Aaron J. Burstein
Outline

1 Research
   - Introduction
   - Model
   - Researchers
   - Summary

2 Survey
   - Introduction
   - Brungs-Jamieson Survey
   - Liles Survey
Introduction

- Computer and Network Security matters have major economic, social, and national security importance
- Present attacks damage machines and disrupt network access
- Attacks continue to grow in numbers
- Information sharing can mitigate attack risk
- It is a constant challenge for research to keep pace with attack vectors
- Sharing data poses considerable privacy risks
- Privacy is protected by the Electronic Communications Privacy Act (ECPA)
- Organizations are reluctant to share their own user data due to privacy issues
- There is limited coordination in the current cybersecurity culture
# Introduction

## National Strategy to Secure Cyberspace
- Encourages firms to share data with researchers
- Protection of privacy and civil liberties

## Privacy
1. Economic and technical components render law enforcement and market based efforts useless
2. Communications privacy law and normals contribute legal roadblocks
3. Data sets are non-existent or unusable for research
4. Require creation of research exceptions and institutional controls

## Security
A computer or network system’s resistance to becoming unusable or attacks that corrupt or leak data
Introduction

2005 FBI Projection
Cybercrime in the U.S. costs 67.2 billion per year

DoD Report
- Forty successful attacks per month
- Tens of thousands of close calls per year

Examples
- 2003 Slammer Worm - Worm spread on the Internet => Shutdown South Korea systems and U.S. ATMs
- 2004 Witty - Worm spread on the Internet => Deleted random data from hosts
- May 2007 Estonia - Massive flood of Internet traffic => Shutdown of banking services
Introduction

**Botnet**
1. Scan network
2. Determine vulnerable hosts
3. Exploit vulnerability
4. Install malware on device
5. Issue remote commands

**Uses**
- Denial of Service (DoS)
- Fraud and Identity Theft
- Spam

**Problem**
- 25% of all PCs with connection are infected
- Malicious activity is not perceptible
- Evasion techniques (anti-virus, logs, and forensic tools)
- Distributed hosts and storage
- Network traces difficult to obtain
Introduction

Economics

- More resources are required to defend attacks
- Production of insecure products
- Adoption of insecure products
- Users lack information and incentive to purchase secure solutions
- Hard to quantify return on investment
- The security practice of one individual can affect the security of others
# Introduction

## Regulation
- Limited direct government intervention
- Copyright - Digital Millennium Copyright Act (DMCA)
- Not seen as primary mean of securing cyberspace
- The Orange Book - Security guidelines for devices and software

## Law Enforcement
- Criminal prosecution is difficult and expensive
- Investigators must secure evidence from multiple sources
- Cooperation is limited and forced with warrants
- Biased priorities for copyright infringement and financial fraud

## Research
- National Science Foundation (NSF), Department of Homeland Security (DHS), Defense Advanced Research Projects Agency (DARPA) by Department of Defense (DoD), Office of Air Force Research, National Security Agency (NSA), National Laboratories (Sandia, Los Alamos, Mitre, Brookhaven, Naval, Army, Ames, Pacific Northwest, NIST)
- Network data sets are critical priority
Outline

1 Research
   - Introduction
   - Model
     - Researchers
     - Summary

2 Survey
   - Introduction
   - Brungs-Jamieson Survey
   - Liles Survey
- ECPA limits acquisition, disclosure, and uses of network data
- Privacy laws prohibit data sources
- Institutional factors inhibit sharing
- ECPA Model for cybersecurity is outdated
- Individuals are equipped to identify and respond to threats on their own systems
- Disclosure of data is allowed to assist in prosecution
- It takes multiple organizations to detect and analyze data properly
- Disclosure exceptions for prosecutions are unfair to research priorities
The Wiretap Act

- Governs the interception of electronic communications
- Enacted in 1968
- Prohibits anyone for intentionally intercepting communications (Governments, ISPs, and Individuals)
- 20 years later blanket statements were added to cover "electronic communications"
- Allows for exceptions (search warrants and statutory)
- Provider exception provides protection for services
Pen/Trap Statute

- Regulates real-time collection of addressing information
- Real-time device installation requires court order
- Providers can install devices to protect users from abuse
- Disclosure of captured data is undefined
The Stored Communications Act (SCA)

- Regulates disclosure of electronic communications
- Covers data-at-rest vs. data-in-transit
- Non-content records (subscriber, IP addresses, email headers)
- URLs and search queries are debatable
- Data freely available to government entities
Examples

July 2002 - RIAA vs. Verizon
- Demanded disclosure of names and other identity information
- Specified particular network addresses assigned at date and time
- Verizon fought the subpoena
- Verizon did not deny the requested data’s existence
- ISPs retain sufficient relational data for several months

Aug 2005 - U.S. DoJ vs. Search Engines
- Due to Child Online Protection Act
- All queries between 06/01/2005 - 07/31/2005
- Google fought the subpoena
- Google argued that queries are trade secret
- Google admitted the queries existence
- AOL, Yahoo, and Microsoft complied with the subpoena
ISPs admit to storing email, pictures, and video messages for a period of time
Disclosure can result in customer backlash
Disclosure can reveal competitive edge in markets
Privacy policies do not directly mention research use
Privacy policies instead emphasize improved service and partner solicitation
Researchers have trouble obtaining data from their own institutions
Competing research and talent acquisition prohibits sharing
Outline

1 Research
   - Introduction
   - Model
   - Researchers
   - Summary

2 Survey
   - Introduction
   - Brungs-Jamieson Survey
   - Liles Survey
Researchers

- Want to advance their research
- Want consistent sharing scheme
- Require access controls and mechanisms for classified or restricted data
- Data should be in RAW format
- Require data sets to persist
- Prefer wide variety of data sources
Examples

<table>
<thead>
<tr>
<th>Lawrence Berkeley National Laboratory</th>
</tr>
</thead>
<tbody>
<tr>
<td>- 11 GB of anonymized network traces (packet headers ONLY)</td>
</tr>
<tr>
<td>- Tried to conceal lab network topology</td>
</tr>
<tr>
<td>- Removed specific types of traffic</td>
</tr>
<tr>
<td>- Believed anonymized be to irreversible</td>
</tr>
<tr>
<td>- Anonymization altered some of the data structure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Aug 2006 - AOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Dataset of 20 million search queries</td>
</tr>
<tr>
<td>- Covered 650,000 users</td>
</tr>
<tr>
<td>- Attempted to anonymize the dataset</td>
</tr>
<tr>
<td>- Within days the New York Times identified one womans queries and published an interview with her</td>
</tr>
<tr>
<td>- Several users sued the company for privacy violations</td>
</tr>
<tr>
<td>- Three employees responsible for the release left the company</td>
</tr>
<tr>
<td>- The research community distanced themselves from AOL and the dataset</td>
</tr>
</tbody>
</table>
1 Research
   • Introduction
   • Model
   • Researchers
   • Summary

2 Survey
   • Introduction
   • Brungs-Jamieson Survey
   • Liles Survey
Summary

- New privacy preserving techniques to allow for better information sharing
- Cybersecurity research and policies have struggled with the question of privacy
- The ECPA security model is outdated and needs to be updated or replaced
- Improvements are made possible by coordinated information sharing
- Research should be allowed similar statute exceptions
- Government has made little to no progress in addressing cybersecurity and privacy
- Industry wants to avoid public disclosure
- Current focus seems to be on data persistence instead of information sharing
1 Research
- Introduction
- Model
- Researchers
- Summary

2 Survey
- Introduction
- Brungs-Jamieson Survey
- Liles Survey
A Survey of the Legal Issues Facing Digital Forensic Experts

*Sydney Liles, Marcus Rogers, and Mariaane Hoebich*
Outline

1 Research
   - Introduction
   - Model
   - Researchers
   - Summary

2 Survey
   - Introduction
   - Brungs-Jamieson Survey
   - Liles Survey
Introduction

Purpose

- Present digital evidence in legal proceedings
- Techniques used to extract evidence must comply with legal standards
Introduction

Purpose

- Present digital evidence in legal proceedings
- Techniques used to extract evidence must comply with legal standards

Problem

1. Investigations are not constrained by geographical boundaries
2. Legal issues are complicated due to the presence of multiple jurisdictions
Introduction

Purpose
- Present digital evidence in legal proceedings
- Techniques used to extract evidence must comply with legal standards

Problem
1. Investigations are not constrained by geographical boundaries
2. Legal issues are complicated due to the presence of multiple jurisdictions

Example
An electronic crime initiated in Australia can bring down a system in the United States
# Introduction - Jurisdiction

## Questions

- Where did the crime occur?
- Which agency has authority to investigate and prosecute?
Introduction - Jurisdiction

Questions

- Where did the crime occur?
- Which agency has authority to investigate and prosecute?

Related Issue: International Cooperation

- Victims can have many different locations
- Trails of evidence can cross multiple national boundaries

Good News

No new cyber crime laws are required. However, existing laws need refinement in terms of definition and clarification.
Introduction - Jurisdiction

Questions
- Where did the crime occur?
- Which agency has authority to investigate and prosecute?

Related Issue: International Cooperation
- Victims can have many different locations
- Trails of evidence can cross multiple national boundaries

Good News
No new cyber crime laws are required. However, existing laws need refinement in terms of definition and clarification.
Introduction - Presentation

- Lawyers, Judges, and Juries have limited technical knowledge
- The presentation of evidence must be done in clear understandable manner
- Legal professionals lack confidence in the producibility of admissible evidence
- No best practice guides are currently available
- The error or testing results for forensic tools are unknown
- The qualifications for expert witnesses are questionable (Does the ability to use an undocumented tool qualify you as an expert?)
Outline

1 Research
   - Introduction
   - Model
   - Researchers
   - Summary

2 Survey
   - Introduction
   - Brungs-Jamieson Survey
   - Liles Survey
Brungs-Jamieson Survey

Overview
- Evaluated attitudes and priorities of the Australian forensic community
- Identified 17 legal issues

Three categories
1. Judicial
2. Privacy
3. Multi-jurisdictional

Goals
1. Identify a set of legal issues facing digital forensics
2. Determine the importance of the identified issues to three stakeholder groups (Police, Regulators, and Consultants)
Brungs-Jamieson Survey

Delphi Methodology
- Is a structured communication, and systematic forecasting technique that relies on a panel of experts
- Experts answer questionnaires over the course of two or more rounds
- After each round results are summarized and anonymized
- This process repeats until the round limit, consensus, or stability is reached
- The final results are in the form of mean and median scores

Ranking and Rating
1. Ranking: 1 (Highest) to 17 (Lowest)
2. Rating: 1 (Unimportant) to 7 (Very Important)
Brungs-Jamieson Survey - Top 5

1. Jurisdictional
2. Telecommunications Act covering data
3. Interpretation of Telecommunications Act
4. International cooperation in practice
5. Revision of mutual assistance
Outline

1 Research
   - Introduction
   - Model
   - Researchers
   - Summary

2 Survey
   - Introduction
   - Brungs-Jamieson Survey
   - Liles Survey
Liles Survey

Overview

- Extension of Brungs-Jamieson Survey (same 17 legal issues)
- Evaluated attitudes and priorities of the United States forensic community

Goals

1. Determine the importance of the identified issues to five stakeholder groups (Law Enforcement, Academics, Government, Industry, and Legal Experts)
Liles Survey - 17 Issues

1. Jurisdictional (state to state and federal to state)
2. Computer evidence presentation difficulties
3. Criminal prosecution vs. civil litigation
4. International cooperation in legal practice
5. Access and exchange of information
6. Confidential records and business system privacy
7. Privacy protection for data transmission laws
8. Privacy issues and workplace surveillance
9. Interpretation of laws affecting digital evidence
10. Preservation of privacy of clients during digital investigations
11. Launching actions against persons unknown in civil litigation
12. Requirement for best practices guides and standards
13. Computer literacy in the legal sector
14. Contrast of broadcast vs. communications
15. Need to specify new offenses
16. Testing of new tools and techniques
17. Expert witness skills and qualifications
Liles Survey

Methodology

- Voluntary and anonymous web-based survey
- Hosted by Center for Education and Research in Information Assurance and Security (CERIAS) at Purdue University from October 26th, 2007 to November 20th, 2007
- Invites were sent to research authors, companies, government, and universities

Ranking

1. Ranking: 1 (Not Important) to 5 (Most Important)
Liles Survey

Participation (Total = 71)
- 13 - Law Enforcement
- 26 - Academics
- 9 - Government
- 3 - Legal Experts
- 20 - Industry

Normalization
- 2 respondents were eliminated due to extreme answers (71 => 69)
- Issue 11 was eliminated due to confusion (17 => 16)
## Liles Survey - Results

**Table 1.** Kruskal-Wallis test results.

<table>
<thead>
<tr>
<th>Issue</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Jurisdictional</td>
<td>41.15</td>
<td>31.64</td>
<td><strong>43.83</strong></td>
<td>21.83</td>
<td>33.11</td>
</tr>
<tr>
<td>2 Presentation Difficulties</td>
<td>32.88</td>
<td>40.30</td>
<td>41.39</td>
<td>12.00</td>
<td>20.08</td>
</tr>
<tr>
<td>3 Criminal vs. Civil</td>
<td>31.15</td>
<td>38.00</td>
<td>32.28</td>
<td>28.67</td>
<td>35.97</td>
</tr>
<tr>
<td>4 International Cooperation</td>
<td>42.04</td>
<td>39.24</td>
<td>33.11</td>
<td>39.33</td>
<td>24.82</td>
</tr>
<tr>
<td>5 Access and Exchange Information</td>
<td>29.46</td>
<td>32.66</td>
<td>24.61</td>
<td>34.00</td>
<td><strong>46.95</strong></td>
</tr>
<tr>
<td>6 Confidential Records</td>
<td>31.31</td>
<td>32.88</td>
<td>33.67</td>
<td>48.33</td>
<td>38.84</td>
</tr>
<tr>
<td>7 Data Transmission Privacy</td>
<td>41.46</td>
<td>33.50</td>
<td>32.72</td>
<td>41.00</td>
<td>32.68</td>
</tr>
<tr>
<td>8 Work Surveillance</td>
<td>32.92</td>
<td>38.80</td>
<td>40.67</td>
<td>40.67</td>
<td>27.84</td>
</tr>
<tr>
<td>9 Interpretation of Laws</td>
<td>33.54</td>
<td>33.12</td>
<td>40.67</td>
<td><strong>60.00</strong></td>
<td>31.84</td>
</tr>
<tr>
<td>10 Client Privacy</td>
<td>27.31</td>
<td>40.60</td>
<td>26.83</td>
<td>37.50</td>
<td>36.37</td>
</tr>
<tr>
<td>12 Best Practices</td>
<td><strong>43.08</strong></td>
<td>34.94</td>
<td>25.11</td>
<td>41.67</td>
<td>33.18</td>
</tr>
<tr>
<td>13 Literacy in Legal Sector</td>
<td>32.31</td>
<td>37.40</td>
<td>27.28</td>
<td>57.50</td>
<td>33.79</td>
</tr>
<tr>
<td>14 Broadcast vs. Communications</td>
<td>33.85</td>
<td><strong>41.24</strong></td>
<td>34.67</td>
<td>7.00</td>
<td>32.16</td>
</tr>
<tr>
<td>15 New Offenses</td>
<td>38.15</td>
<td>33.72</td>
<td>34.44</td>
<td>19.33</td>
<td>27.36</td>
</tr>
<tr>
<td>16 Testing of New Tools</td>
<td>31.19</td>
<td>35.86</td>
<td>37.94</td>
<td>22.33</td>
<td>37.08</td>
</tr>
<tr>
<td>17 Expert Witness</td>
<td>27.04</td>
<td>38.66</td>
<td>34.33</td>
<td>38.17</td>
<td>35.45</td>
</tr>
</tbody>
</table>

**Groups**

2 = Law Enforcement, 3 = Academic, 4 = Government, 5 = Legal Experts, 6 = Industry

*Graphic from A Survey of the Legal Issues Facing Digital Forensic Experts, Sydney Liles, Marcus Rogers and Marianne Hoebich*
## Liles Survey - Results

### Table 2. Comparison of Kendall’s W test results.

<table>
<thead>
<tr>
<th>Issue</th>
<th>Law Enforcement</th>
<th>Government</th>
<th>Commercial</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Liles</td>
<td>B-J</td>
<td>Liles</td>
</tr>
<tr>
<td>Jurisdictional</td>
<td>7.88(8)</td>
<td>7.00(5)</td>
<td>7.00(5)</td>
</tr>
<tr>
<td>Presentation Difficulties</td>
<td>8.50(9)</td>
<td>5.67(3)</td>
<td>6.33(3)</td>
</tr>
<tr>
<td>Criminal vs. Civil</td>
<td>11.50(15)</td>
<td>10.67(14)</td>
<td>11.78(15)</td>
</tr>
<tr>
<td>International Cooperation</td>
<td>6.85(4)</td>
<td>5.33(2)</td>
<td>7.72(9)</td>
</tr>
<tr>
<td>Access and Exchange Information</td>
<td>9.27(11)</td>
<td>6.00(4)</td>
<td>10.94(13)</td>
</tr>
<tr>
<td>Confidential Records</td>
<td>7.08(5)</td>
<td>10.33(12)</td>
<td>6.67(4)</td>
</tr>
<tr>
<td>Data Transmission Privacy</td>
<td>5.23(2)</td>
<td>10.00(10)</td>
<td>7.56(7)</td>
</tr>
<tr>
<td>Work Surveillance</td>
<td>9.23(10)</td>
<td>7.33(7)</td>
<td>7.50(6)</td>
</tr>
<tr>
<td>Interpretation of Laws</td>
<td>6.73(3)</td>
<td>4.33(1)</td>
<td>4.89(1)</td>
</tr>
<tr>
<td>Client Privacy</td>
<td>9.99(12)</td>
<td>10.00(10)</td>
<td>10.06(12)</td>
</tr>
<tr>
<td>Best Practices</td>
<td>5.08(1)</td>
<td>11.00(15)</td>
<td>9.33(11)</td>
</tr>
<tr>
<td>Literacy in Legal Sector</td>
<td>7.42(7)</td>
<td>9.33(9)</td>
<td>8.94(10)</td>
</tr>
<tr>
<td>Broadcast vs. Communications</td>
<td>12.50(16)</td>
<td>7.00(5)</td>
<td>12.33(16)</td>
</tr>
<tr>
<td>New Offense</td>
<td>11.46(14)</td>
<td>10.33(12)</td>
<td>11.33(14)</td>
</tr>
<tr>
<td>Testing of New Tools</td>
<td>7.35(6)</td>
<td>8.67(8)</td>
<td>6.00(2)</td>
</tr>
<tr>
<td>Expert Witness</td>
<td>9.99(13)</td>
<td>3.33(16)</td>
<td>7.61(8)</td>
</tr>
</tbody>
</table>

*Graphic from A Survey of the Legal Issues Facing Digital Forensic Experts, Sydney Liles, Marcus Rogers and Marianne Hoebich*
Liles Survey - Results

- Results not normally distributed
- Non-parametric statistical tests were required
- One-to-one comparison of results was not possible
- Two additional legitimate stakeholders eliminated (Academic and Legal Experts)
- Results differ due to sample size and geographical location
- Stakeholder groups disagree on the importance of legal issues
- Identifying common ground will allow for new policy and funding priorities