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.

Research

Toward a Culture of Cybersecurity Research

Aaron J. Burstein
National Strategy to Secure Cyberspace
- Encourages firms to share data with researchers
- Protection of privacy and civil liberties

Privacy
- Economic and technical components render law enforcement and market based efforts useless
- Communications privacy law and norms contribute legal roadblocks
- Data sets are non-existent or unusable for research
- 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

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

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
- Research
  - Introduction
  - Model
  - Researchers
  - Summary
- 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
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 06/31/2005 - 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
Competing research and talent acquisition prohibits sharing
Research

Introduction

Model

Researchers

Summary

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

Survey

- Data should be in RAW format
- Require data sets to persist
- Prefer wide variety of data sources

Examples

Lawrence Berkeley National Laboratory

- 11 GB of anonymized network traces (packet headers ONLY)
- Tried to conceal lab network topology
- Removed specific types of traffic
- Believed anonymized data to be irreversible
- Anonymization altered some of the data structure

Aug 2006 - AOL

- Dataset of 20 million search queries
- Covered 650,000 users
- Attempted to anonymize the dataset
- Within days the New York Times identified one woman's queries and published an interview with her
- Several users sued the company for privacy violations
- Three employees responsible for the release left the company
- The research community distanced themselves from AOL and the dataset

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
A Survey of the Legal Issues Facing Digital Forensic Experts

Sydney Liles, Marcus Rogers, and Mariamee Hoebich

Introduction

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

Problem
- Investigations are not constrained by geographical boundaries
- 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

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.

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 tool are unknown
- The qualifications for expert witnesses are questionable (Does the ability to use an undocumented tool qualify you as an expert?)
Brungs-Jamieson Survey

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

Three categories:
- Judicial
- Privacy
- Multi-jurisdictional

Goals:
- Identify a set of legal issues facing digital forensics
- Determine the importance of the identified issues to three stakeholder groups (Police, Regulators, and Consultants)

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

Liles Survey

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

Goals:
- 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 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. Launching actions against persons unknown in civil litigation
11. Requirement for best practices guides and standards
12. Computer literacy in the legal sector
13. Contrast of broadcast vs. communications
14. Need to specify new offenses
15. Testing of new tools and techniques
16. 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
- Ranking: 1 (Not Important) to 5 (Most Important)

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)

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

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