Cyber Attack Investigative Tools and Technologies

Kevin O’Shea
Technical Analysis Group
Institute for Security Technology Studies at Dartmouth College
Hanover, NH
For more information:

koshea@ists.dartmouth.edu

www.ists.dartmouth.edu
603-646-0700
ISTS is located at an academic institution in Hanover NH.
ISTS’s core purpose: research and development

- “serve as a center for counterterrorism technology research, development, testing and evaluation (RDT&E) with a particular focus on cyber-security and protection of telecommunications and critical information infrastructure”

  Senate Appropriations Committee Report on H.R. 4690, Department of Commerce, Justice, and State, the Judiciary and Related Agencies Appropriations Bill, 2001 (U.S. Senate, September 8, 2000)

- “serve as a national point of contact for antiterrorism information sharing among Federal, State and local preparedness agencies, as well as private and public organizations”

  Department of Commerce, Justice, and State, the Judiciary and related agencies Appropriations Bill 2001 and the Congressional record (House of Representatives, November, 1999)
Technical Analysis Group (TAG): Mandate

1. Produce strategic analytical reports in critical areas not currently addressed by other national resources
2. Research and test a prototype national contact database for cyber attack investigators
3. Complete the ISTS’s mission to produce a national research and development agenda in the specific area of investigative tools and technologies for cyber attack investigators
• Cyber Attacks: computer-to-computer attack that undermines the confidentiality, integrity, or availability of a computer or information resident on it.
National Research & Development Agenda for Cyber Attack Investigative Tools and Technologies
Problem Statement

- The tools and technologies available to law enforcement are not keeping pace with the advances made by attackers.
- Knowledge of and use of tools is not homogenous across LE communities.
Objective:

- Identify the problems and technological impediments facing law enforcement when investigating and responding to cyber attacks
Study Findings

- Preliminary Investigation and Data Collection
- Data and Log Analysis
- IP Tracing and Real-time Interception
- Emerging Technologies Requiring Research and Development
- National Data and Information Sharing
- Law Enforcement Specific Development Issues
- Training
Preliminary Investigation and Data Collection

- Collection of data from multiple operating systems
- Mapping network topology
- Digital evidence recovery
- Capturing resident memory data
- Analyzing excessively large media storage devices
Data and Log Analysis

• Log compilation
  – recognize and import logs across multiple platforms
  – correct for errors in time stamping and place events into an organized timeline

• Log analysis and reporting
  – perform analysis on the logs
  – have the ability to be linked to other services, such as exploit signature databases
IP Tracing and Real-time Interception

• IP tracing
  – policy and other non-technological issues

• Real-time interception of digital data
  – available technologies were reported to be too complex to implement and use
Emerging Technologies

- Encryption
- Wireless technologies
- Steganography
- Magnetic microscopy
- Forensic data archiving

Institute for Security Technology Studies
at Dartmouth College
National Data and Information Sharing

- Cyber attack profile database
- Virus and worm signature database
- Attack tool signature database
- Law enforcement cyber attack contact database
- Legacy hardware and software database
Law Enforcement Specific Development Issues

- Skill levels
- Investigative support tools
- Help files
Training

• Training is critical to successfully investigate cyber attacks
• Training programs that fit law enforcement (i.e. in service training blocks)
• National initiatives should be undertaken to:
  – Benchmark current training programs, identify gaps
  – Create a national training strategy for cyber attack investigators, prosecutors, and the judiciary
  – Benchmark distance learning solutions for LE use
Next Steps

• Follow on research:
  – Assess existing solutions
  – Perform gap analysis
  – Define gaps and initiate targeted research
The Gap Analysis is the second step towards a national R&D agenda for LE cyber attack investigative tools and technologies

- **Primary:**
  - Identify technology gaps where future R&D may be initiated

- **Secondary:**
  - Establish internal knowledge base & tech capabilities to produce LE tools
### 1. Preliminary Investigation and Data Collection

<table>
<thead>
<tr>
<th>Tool Name</th>
<th>Operating Systems</th>
<th>Network Mapping</th>
<th>Digital Evidence Recovery</th>
<th>Memory Res Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>NeWitness (p/n)</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ProcDiscover DFT V2</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>PATHFINDER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SilentRunner</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Byte Back</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detective</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>White Glove</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log Management Sys</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shadow</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12 Analysts Notebook/Base</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EagleCheck</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Operating systems columns indicate tools that can extract data from operating systems.*

*Network mapping columns indicate tools that can map network topologies.*

*Digital evidence recovery columns indicate tools that can recover digital evidence.*

*Memory res tools columns indicate tools that can recover memory data.*
Preliminary “Policy” Findings

- The universe of cases involving a computer (used in, at the scene of, or the target of a crime) is increasing exponentially.
- Current laws have not kept pace with technological advancements – specifically jurisdictional boundaries, rules of evidence, and forensic storage.
- The probability of successfully prosecuting a cyber attack crime is low.
Software Development for LE

- LE is not seen as a large market for high return ($$) specialized software development
- LE specific development requirements for software (transparent architecture, courtroom support, etc.) conflict with good business practices
- Tool use by LE not proportionate to number and types of tools available
No One Can Be Told What the Matrix Is…

The following “Needs” are under-represented in the Matrix:

• Help present complex computer crime related case information to a judge and jury in court
• Capability to detect IP spoofing
• Search a network to retrieve logs
• Captures RAM resident data
What the Matrix is telling us con’t:

- Provides LE with added capability to circumvent encrypted data
- Recover data deleted / wiped / or off of damaged drives, i.e. magnetic microscopy
- Database of virus / worm / cyber attack tools and code accessible to LE
- Legacy hardware clearinghouse
Then what?

- Frame the National R&D Agenda
- Methodology
  - National decision maker / subject matter expert level meeting to prioritize research areas identified in the gap analysis
  - Working meeting with the resulting material drafted into the ISTS National R&D agenda
Information Collection and Analysis

- National Resource
- Mirrored by the SANS Institute
- Over 2000 subscribers

http://news.ists.dartmouth.edu/todaysnews.html