System Assessment and Validation for Emergency Responders

# Summary

SAVER

September 2004

## Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Research and Development Agenda

### SAVER Summary of the Following Report:

Institute for Security Technology Studies, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Research and Development Agenda* (Hanover, NH: Trustee of Dartmouth College, 2004).

While cyber-attacks on government, corporate, and academic networks have increased in both severity and sophistication, the technological tools used by law enforcement during investigations has failed to develop at the same rate as the evolving instruments employed by attackers. Consequently, the Technical Analysis Group at the Institute for Security Technology Studies, through a multi-year research effort, conducted three national studies to identify, analyze, and prioritize the technology needs of cyber-attack investigators and prosecutors. The first study, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: National Needs Assessment* (available at: http://www.ists.dartmouth.edu/TAG/lena.htm), looks at the problems and technological impediments facing federal, state, and local law enforcement when investigating and responding to attacks. The second study, *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: Gap Analysis Report* (available at: http://www.ists.dartmouth.edu/TAG/gap_analysis.htm), determines which problems were not satisfied by the existing available technology solutions that claimed to meet the requirements revealed in the *National Needs Assessment* study. *Law Enforcement Tools and Technologies for Investigating Cyber Attacks: A National Research and Development Agenda* (available at: http://www.ists.dartmouth.edu/TAG/randd.htm), the third study, prioritizes the major problems encountered during cyber-attack investigations, for which research and development might provide solutions. The National Research and Development Agenda is the culmination of the research and analysis conducted during all three studies and is based on data collected and analyzed from September 2001 to December 2003.

SAVER Program
Phone: 877-347-3371 Fax: 443-402-9489
E-Mail: saver.odp@dhs.gov
Web: http://www.dhs-saver.info

SAVER is sponsored by the U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness

This project was funded under Grant #2003-TK-TX-0002 from the Office of State and Local GOvernment Coordination and Preparedness, Systems Support Division (OSLGCP SSD), U.S. Department of Homeland Security.

Opinions or points of view expressed in this document are those of the authors and do not necessarily represent the view or official position of the U.S. Department of Homeland Security, Office of State and Local Government Coordination and Preparedness, Systems Support Division.

## The Investigative Process: Preliminary Investigation and Data Collection

*"There is a need for easy-to-use search functions that would detect patterns and anomalies from collected log files. "*

Timely data collection is essential to a cyber-attack investigation. Ideally, the victims would detect and report an attack while in progress, making the recovery and collection of logs and other data easier to obtain. Realistically, investigators are notified after an attack when the collection process becomes more difficult or even impossible to complete. The current collection process is often done manually. Automating the identification and collection of relevant case data before it is no longer available would significantly increase law enforcement's ability to investigate an attack. However, locating log files is becoming increasingly more complicated as they are written across network area storage and filed remotely in organizations with geographically separated offices. Furthermore, devices present on modern computer networks, and the operating systems running on the devices, are often from different manufacturers, and investigators must be able to collect and correlate relevant data from any operating environment. The *National Needs Assessment* reports a need for technology solutions to search a network for logs, recognize the locations where log files are kept, and collect them regardless of the platform or format of logs on a computer. In addition, when new and updated systems are introduced, the challenges of collecting log files will become more complicated, making it imperative that technology keep pace while the formats of files and programs change. Although a significant number of tools were identified, cyber-attack investigators indicated the current software may be too expensive, complex, and lack specific functionality. The automation of processes that are currently undertaken manually and the problems with expedient collection of data from multiple operating systems must be addressed.

When an attack is reported, investigators speak to parties responsible for computer security. Network system administrator(s), in-house investigator(s), and external security consultant(s) often assist investigators with the location and retrieval of appropriate log files and related data. When administrators or other insiders are not available, finding relevant log files on unfamiliar computers and networks can become a very time consuming process. The situation is further complicated as the insiders could be suspect, unskilled, or provide incomplete data. Therefore, data collection tasks must be questioned where the quality or integrity of involvement by in-house staff is concerned. Solutions that help minimize insider involvement would greatly improve the investigative process.

Digital evidence recovery tends to focus on recovering data written to a magnetic medium. In some situations hard drives or entire computers are seized creating a problem with obtaining transient data from the computer's memory. Volatile resident memory data may only be obtained from a computer that is turned on. When a computer is turned off, the data stored in the Random Access Memory (RAM) is usually lost. Investigators face further challenges in software that is designed to run primarily in RAM. The *Gap Analysis Report* discovered no tools that purported to capture memory-resident data. Furthermore, capturing memory-resident data without modification may not be practical since solutions may change the data upon execution. New technology solutions should provide consistent, reliable, and auditable actions so that any variations in data caused by the tools would be clearly identifiable.

In *National Needs Assessment*, investigators outlined the need to quickly and accurately determine the logical and physical topology of a victim's network during beginning stages of a cyber-attack. A critical component is the ability to recognize and detect the numerous devices that are present on the network. The process of mapping the logical and physical relationships is often manual. Network management tools are available, but they do not meet requirements, as they are often designed for installation by system administrators as part of their network management function, and are not tailored to investigative purposes. Furthermore, these tools often require pre-installation before an event occurs and are priced too high. Investigators are in need of tools that will alleviate dependence

on insiders during data collection, have the ability to run autonomously or with minimal specialized training for investigators, and include graphically represented results for both the physical and logical arrangements of a network, as each lends itself to different investigative techniques.

The ability to analyze very large data sets also presents a problem to investigators. The cost of large capacity data storage devices continues to drop with no corresponding advance in technology to assist in the collection, analysis, or storage of large data sets. The *Gap Analysis Report* identified many tools that claim they are designed to examine large data sets but current software is not meeting investigator's needs. The current tools are designed for forensic work in traditional crimes, and for use on individual computers, but not across networks. Also, the rapidly increasing size of digital storage devices is outstripping current software's ability to process the data in a timely manner when investigators must complete multiple tasks with multiple computers. It often takes hours or days to complete the analytical processes.

## The Investigative Process: Log Analysis

Log files may provide information on when a cyber-attack happened and how the attacker gained entry to the compromised system. It is not uncommon for different sets of logs to be generated on a number of devices (web server, mail server, or file server) within a network. Administrators usually maintain logs for normal operational tasks, but operational and audit logs may not contain enough detail. Consequently, logs investigators work with often contain limited data. Increasing the amount and type of data captured in log files significantly increases the chance of discovering and tracking unauthorized activity. The fact that attackers may erase or modify log files to mask illicit operations makes the task of uncovering

*"Ideally, the victims would detect and report an attack while in progress, making the recovery and collection of logs and other data easier to obtain."*

activity even more difficult. Thus, log file analysis is critical and complex and requires training and experience. The analysis is a time consuming process, and is often done manually, or with the use of simple sorting and editing programs. Therefore, investigators need better solutions to search, collect, and compile logs regardless of platform or format. Solutions that package logs into a common portable format would allow investigators to broadly share information.

Log analysis solutions should also present detailed technical information in a graphical format. There is a need for easy-to-use search functions that would detect patterns and anomalies from collected log files. Many of the data files gathered and produced during an investigation are in the form of detailed lists of events, network connectivity descriptions, and other numeric and character data. Visualization may reduce the time needed to understand how an attack occurred. Furthermore, time and date stamps across computers in different time zones need correcting, and automated tools that compile and present time-corrected logs on a graphical timeline would be helpful. While some tools were identified as presenting data in a graphical format, their cost was beyond most agencies. Besides, the tools were designed for criminal activity analysis, and it is unclear if they would be useful for cyber attack data. A final factor calling for graphical representation of log analysis is the need of prosecutors to show the development of an attack, or the progression of an attack through a network, while simultaneously explaining technical issues, in court.

## The Investigative Process: IP Tracing and Real-Time Interception

Internet Protocol (IP) addresses help investigators to trace the origins of cyber attacks. However, cyber attackers routinely use software specifically created to change their IP address to conceal their identity or the origin of an attack. The *Gap Analysis Report* shows that there are tools that may be useful, but they are often the same tools used by attackers and are not designed for investigations. Available tools are principally freeware or embedded capabilities in operating systems.

Concerning real-time interception, the need to differentiate between those under surveillance and others on the network is an increasing problem. In instances where digital interception is warranted and legally authorized, local and state agencies have found themselves without the necessary technology, or in possession of technology that exceeds their level of training. Telecommunications venders may provide solutions that can identify, isolate, copy, and record transmissions in real-time but costs may be prohibitive. Of the existing tools available, many are installed by systems administrators for network management, and are not forensic tools by design; they often require pre-installation.

## Emerging Technologies Requiring Research and Development

Many technologies such as encryption and steganography are already impacting investigations and demand immediate attention. Criminals employ freely available, strong encryption technologies. Currently investigators use "work arounds" or technical means to circumvent encryptions: witness cooperation, password text within another file, keystroke logger programs. The outright defeat of encryption may not be a reasonable short-term research goal but may be a primary focus of mid- to long-term research efforts.
Digital steganography is a term used to describe techniques for hiding data within a digital file in such a way that it is difficult to discern the presence or contents of the hidden data. The techniques employed in steganography may make no perceptible change to the source file. Further, many steganography programs employ encryption as an added layer of security. Currently, the detection is generally limited to searching for the programs used to create steganography files, but many can run from a floppy, a USB drive, or RAM, and leave no trace in the system after use.

## National Information Sharing

A recurring theme during the research behind these reports is the need for information sharing services pertaining to cyber-attack

investigations. Multiple agencies may be working independently on cyber attack cases that all originate from a single attacker. Investigators would welcome technological solutions that automate pattern analysis and technical exploit identification across geographic locations to indicate if their case is linked to other investigations. The *Gap Analysis Report* refers to a number of organizational systems that are currently available to investigators to assist in cross jurisdictional communications, but they could benefit from greater coordination.

The entities that develop technological solutions to the problems outlined in this study have a singular opportunity, as the solutions that are developed may become widely adopted by the law enforcement community. Well designed software for law enforcement that integrates users' needs could revolutionize the speed and effectiveness of investigations.

*This SAVER Summary was produced with permission from the Institute for Security Technology Studies in Hanover, NH. The original document was copyrighted by Trustees of Dartmouth College, 2004.*

**For more information** on SAVER, visit the SAVER website at www.dhs-saver.info or call the SAVER Program Office at 877-347-3371.