E-Crime Investigative Technologies

Sudhir Aggarwal, Zhenhai Duan, Leo Kermes, Breno de Medeiros
Computer Science Department, Florida State University, Tallahassee, FL 32306
{sudhir, duan, kermes, breno}@cs.fsu.edu

Abstract

This paper describes three projects that are part of a research agenda in support of digital forensic investigations. The R&D activities involve developing new technologies and forensic tools to address real-world problems related to electronic/digital crime. The three projects are the DNA project, dedicated to cryptanalysis of passwords; the UnMask project, which addresses the issue of automated support for investigation of phishing attacks; and the PAPA project, which was designed to capture interactions with cyberstalkers and perform sting operations. The DNA and UnMask tools are operational and undergoing testing. The testing of the PAPA tool suggested several alternate uses of the system.

1. Introduction

In this paper, we describe the R&D activities of the E-Crime Investigative Technologies Laboratory (ECIT) at the Florida State University. ECIT work currently encompasses a number of research projects, including systems for password and passphrase cracking, techniques for investigating email phishing scams and threats, and tools for combating cyberstalking and investigating online predators.

ECIT collaborates closely with the Florida Department of Law Enforcement and the National White Collar Crime Center and partners such as AccessData Corporation. The goal is to build novel systems for E-crime investigations. The mechanism of developing projects is: (1) brainstorming with law enforcement agents and others to determine law enforcement investigative needs; (2) exploring novel technologies to be used in support of the resulting requirements; and (3) developing prototype systems and tools that can be used in investigations.

In this paper we explore these goals through a survey of several projects, touching on requirements and constraints of law enforcement, and on related technology and legal issues.

1.1. General approach

ECIT research takes a very pragmatic approach in building digital forensics systems. We focus on ways to automate tedious processes, improve workflows of investigations, enable collaboration between law enforcement agencies, and facilitate resource sharing.

Research activities in ECIT must be cognizant of the privacy, security and legal concerns involved in investigations, as well as the need for proper evidentiary support for subsequent prosecution and trial.

1.2. Specific projects

The DNA project builds on AccessData Corporation's Distributed Network Attack™ (DNA) commercial product. DNA is a popular tool for decrypting password-encrypted files. ECIT worked with AccessData to develop DNA Online, a web portal to allow law enforcement to securely share a DNA Silo installation over the Internet. In this project, ECIT research activities also explore techniques and tools for breaking passphrases in addition to passwords.

In the UnMask project ECIT is working to develop an automated system for investigating email-based crimes. An email is first parsed to extract relevant components from the email and further information is gathered via automatically launching appropriate UNIX tools such as whois. The resulting information is gathered into a relational database so that reports can be generated and business logic applied through the use of structured queries.

The goal of the PAPA project was to build a system to support law enforcement agents in helping victims of cyberstalking. It allowed agents to "shadow" the victim remotely and provide online guidance while securely capturing and logging data related to the cyberstalking activity.

In Sections 2-4 we discuss DNA, UnMask and PAPA, respectively. In Section 5, we provide some concluding thoughts on building systems to combat E-crime.

2. The DNA Online project

In the process of a forensic investigation, it is not unusual for investigators to encounter encrypted files that might potentially hide evidence of criminal activity. If the suspect is still in use of his computer, it may be possible to place covert key loggers or to use social

1530-1605/08 $25.00 © 2008 IEEE

engineering strategies to compel revelation of the password that protects the encrypting key [14]. If, on the other hand, the computer files have been obtained as a result of executing a search warrant, such methods may no longer be available.

In the latter case, crypto-analytic approaches to recover the encryption key must be used. Moreover, as high-quality tools for encryption have become widely available and are generally inexpensive [8], [14], crypto-analyzing the password that protects the key is often the only viable approach.

2.1. Motivation

Several commercial applications provide cryptanalytic/guessing attack capabilities against passwords. One of them is the PRTK™/DNA™ set of forensic tools developed by AccessData®.

In particular, the DNA™ tool is capable of marshalling network resources to accomplish parallel password guessing, which can dramatically reduce the search time in successful password guessing trials, as password-guessing is a fully parallelizable task [6].

In practice, however, different investigating agencies have unequal capabilities in terms of equipment and trained personnel to use such tools. DNA Online seeks to create a platform for forensic (and more specifically, password-recovery) tasks that enables collaboration between agencies and resource sharing.

This interface should interoperate with one or more DNA™ silos—large networks of computers that are available, perhaps in their idle cycles only, to perform such tasks. Therefore, a well-equipped organization may fully utilize its resources by providing auxiliary services to partner agencies. This host organization should have the ability to prioritize tasks according to its policies and mutual agreements with partners.

2.2. Architecture

In this section, we give an overview of the main features of the DNA Online password-recovery portal. A more detailed description of DNA Online is available in [1].

2.2.1. User Interface. Our prior experience with designing digital forensic tools for use by the general law enforcement community was incorporated into the decision process that guided the design of the DNA Online interface. In particular, we took a deliberate approach to derive functional requirements for the UI, reflecting a few guiding principles.

First, when interacting with law enforcement agents, we focused on understanding their workflow—what is that they need to accomplish. Next, we sought to learn how they organize information (evidence) in the physical world. Finally, we set out to design the simplest, cleanest interface that would be intuitive by capturing the tasks in their workflow and mimicking their information handling practices.

This approach allows us to maintain control of the design definition process, to discover true requirements—as opposed to comprehensive and non-prioritized wish lists—and to strive for a robust development process leading to code that is more reliable, secure, and extensively tested.

An interface snapshot is provided in Figure 1. After logging into the system, the officer has an opportunity to create a new case, or to manage existing ones. A "case" is the logical envelope that organizes one or more password-recovery tasks, represented by a set of submitted file (or file headers), and any contributory information to facilitate password recovery. Examples of such information are: biographic data on the suspect; plaintext information recovered in the suspect's computer, such as e-mail addresses and birthdates, and other similar data. Such information applies to all the password-recovery tasks in the same case—i.e., for the same suspect.

2.2.2. Job management. Within each case, specific password-breaking tasks are called "jobs." We now briefly describe how our DNA Online portal manages the preparation and submission of jobs to the DNA application that actually performs the forensic tasks.

First, if auxiliary biographical-type data is provided, it is parsed into a "dictionary" of terms that relate to the suspect. In addition to biographical data, the agents may also submit URLs of web pages frequently visited by the suspect. These pages may contain non-standard linguistic terms and words from domains or communities of interest to the suspect.

The portal was designed for extensibility, and in the near future it will be capable of, upon receiving a URL, parse the corresponding pages, and extract another "dictionary" of unique words and terms found in the submitted web pages. The case-specific dictionaries are then combined with general-purpose dictionaries, and used to create password-recovery profiles.

These profiles expand the dictionary information by applying to each entry in the dictionary a set of transformation rules. A common strategy is to apply all transformations that can be described by a set of simple regular expressions. For instance, a rule may append two numerical digits at the end of each dictionary entry.

Figure 1. Snapshot of the Case Management System

Once a job profile has been created, the files representing the job target, dictionaries, and the profile are sent to a silo-accessible system hosting a DNA™ supervisor node. From there, the password search space is abstracted as a linear key-space, and the password-recovery task can be parallelized among many client nodes. Figure 2 shows all the system components and their relationships.

In addition to the functional requirements, several security concerns attended the design of DNA Online. Naturally, it was necessary to provide security for the online-accessible user accounts, particular since nearly all the expected content would be sensitive by its very nature.

It was also necessary to preclude creation of accounts by persons not associated with the supported law enforcement agencies—to prevent our tool from being used as a password-breaking utility for hackers, or from diluting the IP rights of our commercial partner, AccessData®.

At first, we thought that our security design could reflect standard practice for secure web applications. We later decided otherwise, based on the fact that submission of jobs to the DNA™ tool required the web server to directly interact with the file system of the host Windows 2003 server. In contrast, most online merchants use web-database connectivity solutions.

The web components were developed in Java to run within the Tomcat servlet. The code is easily portable to a large range of architectures. We deployed it within a Linux box to ensure that standard-compliant communication between the web-server and the DNA™ host was followed, and to provide better isolation of trust. In particular, our design uses the LDAP access control features supported by Windows, with the web server behaving as an (untrusted) remote client in its communication with the DNA™ host.

2.3. Privacy and Legal Concerns

In addition to the aforementioned security issues, there are special considerations about the information submitted by enforcement agencies.

To an extent, several issues related to the acquisition, handling, and admissibility of digital evidence obtained through forensic or investigative procedures have not been fully settled by courts. Only recently, for instance, the 9th District Court of Appeals issued a decision stating that the acquisition of IP addresses in network flows (and the associated volume of traffic) is similar to the process of using pen registers to capture phone numbers dialed, and therefore not protected by the U.S. Constitution's Fourth Amendment, or requiring warranties [9]. This represented the first ruling on this important evidentiary matter at the U.S. District Court level.

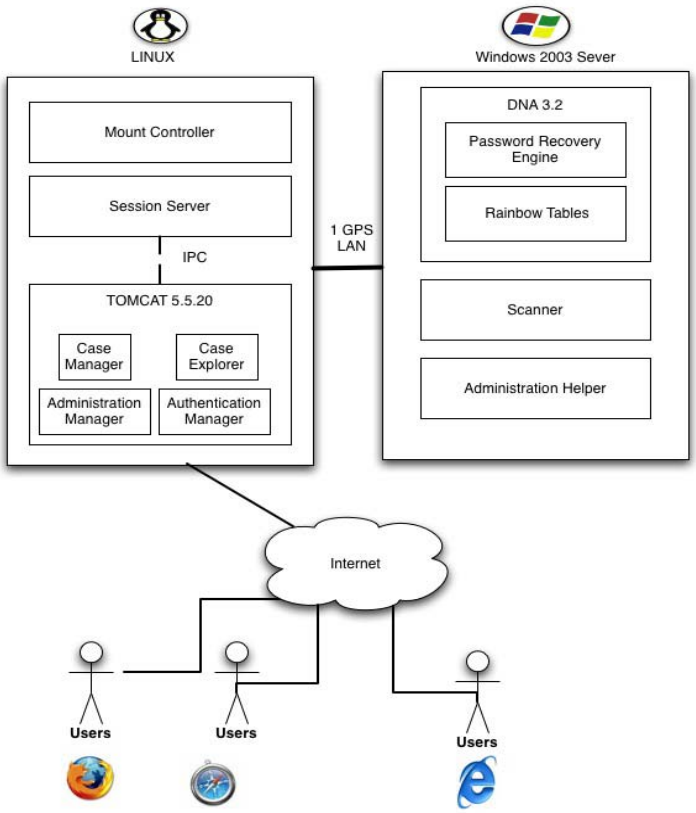

Figure 2. The components of DNA Online

With respect to the operation of the DNA service, it is important to pay heed to the confidentiality protections afforded to evidence prior to it being reviewed and judged admissible (when it typically becomes part of the public domain). Since encrypted files cannot be considered as having been reviewed, their contents should remain private and in possession only of the investigative agencies. However, the same degree of protection may not apply to passwords and keys used to protect private files. Therefore, we have decided to support, and even enforce whenever possible, that submissions include only the first few blocks on information of an encrypted file, i.e., the minimal information needed for a password-breaking attack.

2.4. Evaluation

We have completed initial testing and are moving to a phase of performance benchmarking. We plan to consider load-balancing strategies to optimally utilize several DNA™ hosts connected to the same portal.

The code developed by the project has been made available in the Sourceforge portal (http://sourceforge.net/projects/dnaonline/). We hope to garner feedback on the reliability of the tool by making it universally available for downloading, testing, and improvement by interested parties.

Concurrently with the DNA project reaching a more mature state of development, we have deepened our efforts to interact with law enforcement, and in particular have maintained a dialogue with an FBI detective who has provided us with continuing valuable feedback into usability and relevance of features for the system.

2.5. Future work

In future work, we plan to extend the DNA Online portal concept as a platform for access to multiple forensic tools. This will involve integrating the existing approaches in DNA Online and UnMask projects, and generalizing the solution further.

In particular, we hope to migrate to a web-database solution for the portal, and to use stored procedures in the database to allow for transparent interaction between the database and the file system. By making the web functionality and the file system manipulation even more asynchronous than in the current design, we hope to achieve better scalability and robustness at the web server.

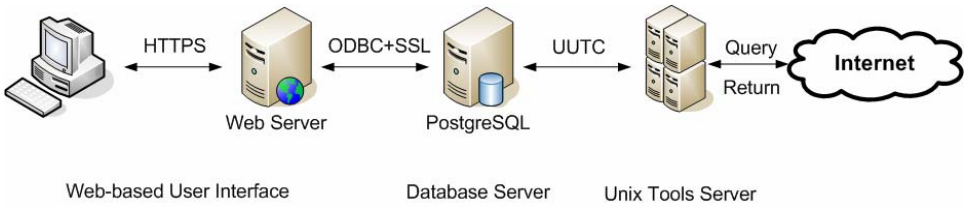

Figure 3. Overview of UnMask architecture

This solution, while more complex in terms of the number of software components, will actually be more in line with standard business approaches and facilitate commercialization and support of the tool as a product.

In addition to supporting law enforcement activities, the DNA project is scheduled to focus more resources in the future into basic research, seeking to increase the effectiveness of current crypto-analytic and password/ passphrase search strategies. We are developing algorithms to generate passwords and passphrases involving novel probabilistic models. To measure the efficacy of the new methods, we have collected several data sources, including a variety of corpuses from popular culture references to serve as dictionaries and lexicon sources for probabilistic password generation. We have also obtained lists of passwords that were compromised (by dishonest parties) through Internet-based attacks. We plan to use these password, following ethical guidelines that guide the use of such sources for research purposes, to obtain measures for the quality of our new algorithms when compared with the state-of-the-art.

3. The UnMask Project

The Undercover Multipurpose Anti-Spoofing Kit (UnMask) that we describe in this section is a software system that supports law-enforcement in investigating email-based crimes such as phishing scams [5].

3.1. Motivation

Phishing scams use emails to drive users to forged websites using technical exploits and social engineering. They trick users into revealing personal data (e.g., passwords, social security numbers and credit cards numbers). Once these data are (illegally) captured, they are typically used for a number of more serious cyber crimes, such as fraud, identity theft and hacking (unauthorized access and theft of services).

Investigation of email-based crimes such as phishing scams by law enforcement often requires a deep understanding of the Internet technologies beyond the email application itself, which are frequently outside of the expertise of law-enforcement investigators.

Law-enforcement agents often perform such investigations manually or semi-manually, based on a recent survey of investigators who spent substantial time doing online investigations involving emails [11]. At the current time, investigating email-based crimes tends to be labor-intensive tasks that produce lots of dead-ends and few tangible results [12], [13], [10].

UnMask automates and facilitates many phases of the investigation of email-based online crimes and it reduces the time and effort needed for digital forensic investigations of such e-crimes. UnMask is a user-friendly system for parsing email header and body and gathering further forensic information associated with the message from the Internet. It can produce an actionable evidentiary trail that law enforcement agents can use to develop viable leads for the cases they are investigating.

An important feature of the UnMask project is that a database serves as a central component that not only keeps track of the initial phishing emails under investigation, but also stores subsequent information searched after deconstruction of the email.

Once the complete forensic information related to an email is obtained, UnMask can generate reports according to the investigation needs of law enforcement. UnMask provides great flexibility in generating reports. In addition to a complete report that includes forensic information of all fields in an email, UnMask can also generate tailored reports for specific fields based on the investigation needs of agents. For example, a report can provide details about the email trajectory, a summary of the content, factual vs. forged IP addresses, pointers, linkages, discrepancies, etc.

In addition to assisting law enforcement in online investigation involving email, UnMask can also be used for forensic investigations of other crimes that use emails as a vector, such as threats and harassment.

To the best of our knowledge, UnMask is the first comprehensive system that can automatically analyze emails and generate forensic reports to be used for subsequent investigation and prosecution.

3.2. Architecture

As shown in Figure 3, an UnMask system consists of three key components: 1) a web-based user interface, 2) a database server, and 3) a UNIX Tools server. In the following, we discuss these components in greater detail.

3.2.1. Web-Based User Interface. UnMask users interact with the system via a web-based user interface. The user interface for UnMask supports a case management system for uploading of email files for analysis.

After logging into the password-controlled UnMask server, the user may submit an email file (in EML format), as part of a new or an existing case. After the email is deconstructed and processed (which we will discuss shortly), the user is able to view the generated reports. UnMask's UI is similar to that of DNA Online, see Figure 1.

3.2.2. Database Server. At the heart of UnMask is a database that glues all the components of the system together. We chose the PostgreSQL database because of its native interfaces for procedural languages, triggers and stored procedures, as well as for its ACID transactional capabilities (*http://www.postgresql.org*).

The database system implements two key functionalities to automate and facilitate the forensic efforts of law-enforcement agencies. First, when a message is submitted via the web interface, the message is fully parsed to obtain all the atomic elements of the message (IETF RFC 2822, *http://www.ietf.org/rfc/rfc2822.txt*).

Through parsing, the raw e-mail is deconstructed, the e-mail header fields and e-mail body are analyzed, and specific components from the email, such as IP addresses or machine domain names, are extracted. The parsers are written in Perl and are based on freely available email and HTML parsing packages from the Comprehensive Perl Archive Network (CPAN, *http://www.cpan.org/*).

These extracted atomic elements, along with the raw submitted message, are stored in the database. Our database is designed to support only append—write once—operations. This maintains evidentiary trail for subsequent prosecution.

When table-record inserts occur, they can initiate other database activities through the use of triggers. Activities can include parsing fields of records in tables, initiating a connection to the UNIX Tools server, and entering new records into tables.

The second functionality of the database server is to instruct the UNIX Tools server to launch the proper forensic tools to collect further information associated with the message. The interaction between the database and the UNIX Tools system is initiated through an innovative use of the "trigger mechanism" of PostgreSQL, in conjunction with a simple protocol called UnMask UNIX Tools Connection (UUTC) that we have designed and implemented between the PostgreSQL database and the UNIX Tools system. This protocol opens a socket connection when needed to a daemon process (the UNIX Tools server) and allows parameters needed for invoking specific tools to be sent across the connection. It also permits return information to be properly put back into the database. Specific tables are used to store data that is returned from actions of the UNIX Tools server.

3.2.3. UNIX Tools Server. The UNIX Tools system runs on a UNIX machine, where it waits for service requests from the database system. The UNIX Tools server provides the basic forensic toolkit for email investigation.

Based on the current common practice of law enforcement in email investigations, the UNIX Tools system provides the following basic functionalities by querying the Internet: 1) mapping between domain names and IP addresses; 2) identifying the DNS and mail servers associated with a domain; 3) identifying the contact information of the person(s) or organization responsible for maintaining an IP address or domain; 4) verifying the validity of email addresses; and 5) reachability of and routes to an IP address or domain.

The flexibility of our design allows other tools to be easily developed and incorporated into the system. Thus, more and more complex investigative tools can be incorporated as they become available.

3.2.4. UnMask report. UnMask provides great flexibility in generating forensic reports. Via the web-based user interface, agents can generate tailored reports based on the needs of investigation.

For example, agents can request a complete report of an email that includes detailed analysis of all fields in the email, or a tailored report of specific fields, email addresses, links in the email.

A (complete) report follows the structure of an email message. Starting with email header information, the report shows the specific header fields isolated for clarity and coupled with information gathered by the UNIX tools. This additional information expands the investigator's understanding of that field.

For example the trace fields "*Received:*" would appear with an analysis of the sending and receiving mail hosts (IP address, domain name, traceroute result, DNS and whois records, etc).

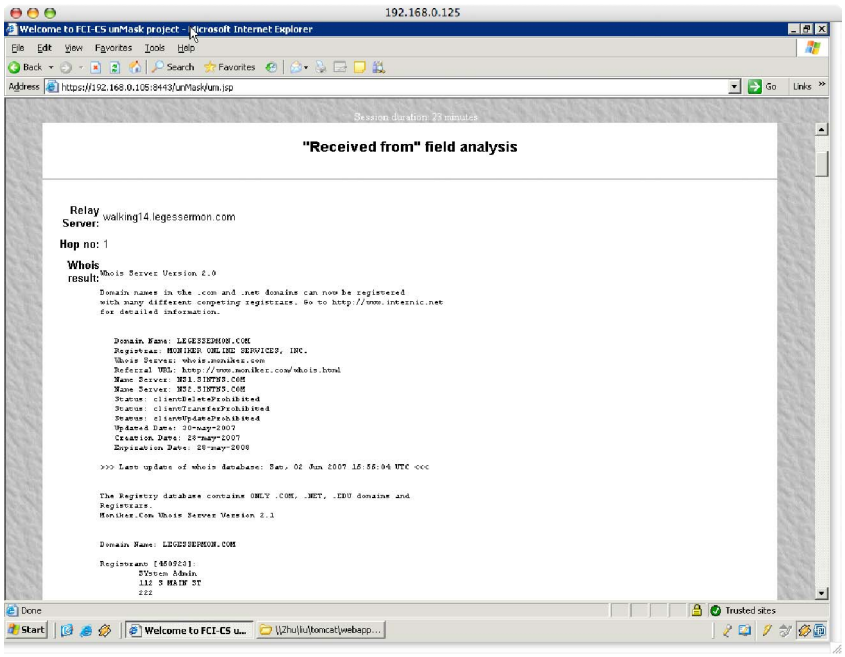

Figure 4. Snapshot of segment 'Received' header field report

This provides the investigator with as much information as possible and aids in the decision making process on what forensic leads to follow further. Figure 4 shows a segment of report related to a "*Received:*" header field in a message that we received.

3.3 Current development status

To ensure the usability of the UnMask system for law enforcement, the ECIT team has been meeting with members of FDLE and NW3C monthly since the beginning of the project. Their feedback and comments provided valuable input to the development of the UnMask project.

The version 1 of the UnMask is a working system, completed except for bullet proofing and hardening of the code. We confirmed its utility by evaluating it against a database of phishing e-mails made available to us by the Anti-Phishing Working Group (APWG, http://www.antiphishing.org/).

We have provided the first version of the system to law enforcement for experimental usage. Using the feedback the investigators provide, we have made a number of improvements over the system. Based on their feedback, we plan to add features and search tools, and increase the facility of investigators in determining the exact information they wish to gather.

3.4 Future work

Given the flexible design of UnMask, many sophisticated logical analyses of the data could be further incorporated into the system. We plan to enhance the system in the following directions.

First, we will incorporate more sophisticated message correlation facilities into the system. Such facilities can cluster messages based on certain desirable features of the messages. Second, we will provide more proactive tools in the investigation and prevention of email-based crimes, for instance, a tool to investigate suspect websites. We also plan to develop techniques and tools to establish the "fingerprints" of various types of phishing messages.

4. The Predator & Prey Alert System

The Predator & Prey Alert System (PAPA) was designed to support law enforcement in monitoring and assisting a cyberstalking victim. An important component was the capability of capturing relevant evidence for subsequent prosecution. Further information on PAPA can be found in [3], [4], [2].

4.1. Motivation

Stalking has been defined as repeated harassment with intent of intimidation or harm [16]. Predators usually know their prey and are deemed mentally normal, but they may also be obsessed [7].

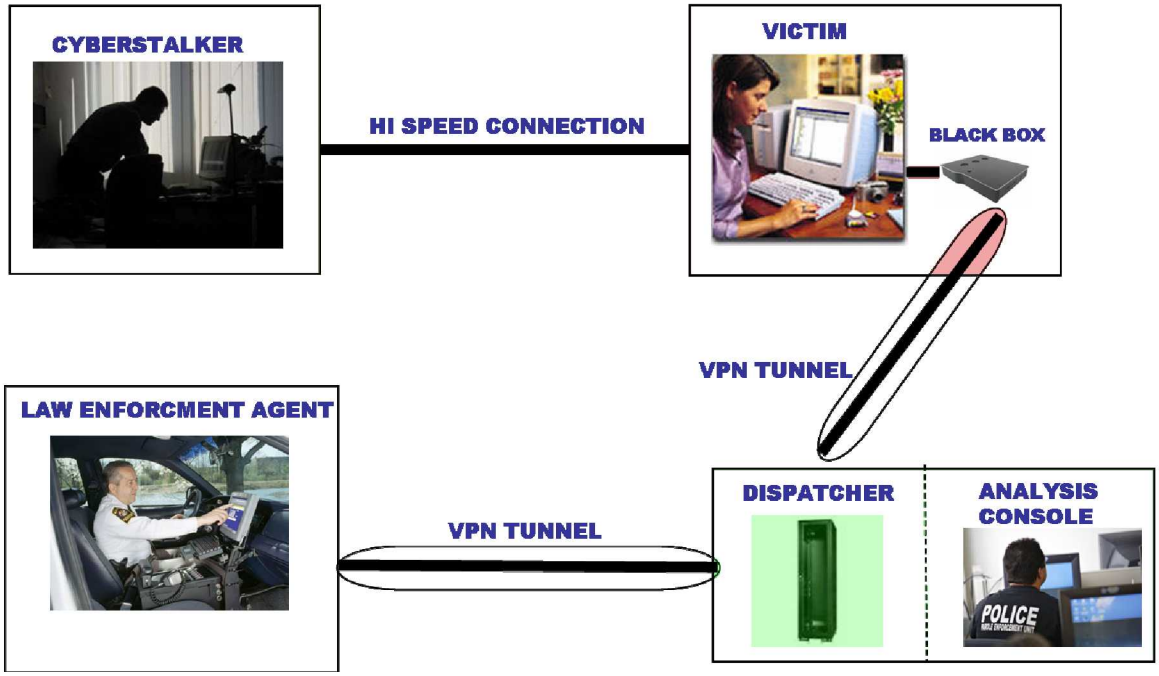

Figure 5. Overview of the PAPA architecture

Cyberstalking is an extension of stalking through the mechanism of the Internet. The (perceived) anonymity of the Internet fostered this new category of stalking, evolving within the technologies of chat rooms, text-messaging systems, and even online network games. Cyberstalking presents several challenges to law enforcement because anonymity emboldens the dynamics of the predator and prey relationship, while making it difficult to trace the true identity of the predator.

The goal of PAPA was to build a set of integrated tools to enable law enforcement to investigate adult cyberstalking where the victim wishes assistance from law enforcement. It allows the capture, index, and replay of evidence of the victim's interaction with a stalker. A primary feature of the system allows "shadowing" of the victim by an agent, i.e., a connection to the victim's computer to view exactly what the victim is observing.

The system requires a secure trust boundary so that a chain-of-custody for evidence can be established. It uses a secure VPN connecting the machines to implement a secure channel between victim and law agent.

A prototype system was built with subsequent feedback collected from law enforcement. This led us to re-evaluate the goals of PAPA and to a decision to pursue a revised system. This recently proposed system is discussed in Section 4.5.

4.2. Architecture

The design of the PAPA system includes both software and custom hardware, primarily in order to be low-cost and also because of the desire to use only open source components. The basic architecture of the PAPA system is captured in Figure 5.

The basic functionality of the PAPA system permits a remote agent at to record evidence of a cyberstalking attack. The Victim Software Module resides on the Victim's computer and provides various capabilities for the victim, such as starting and stopping the recording of the session and tagging important parts of the session.

The Agent Module allows law enforcement to view exactly what the victim sees in a window on the agent's machine, and dialogue with the victim through a separate chat channel.

The Session Recorder (termed a black box in the figure) is connected to the victim's machine and interfaces both to the upstream connection to the cyberstalker, as well as to the dispatcher. The Session Recorder is a custom-built portable hardware device that records two-way exchanges between the agent-victim and victim-predator; preserves the integrity of the evidence with access control techniques and optional encryption; and coordinates network communications between the victim's computer and law enforcement systems by means of a discreet second channel.

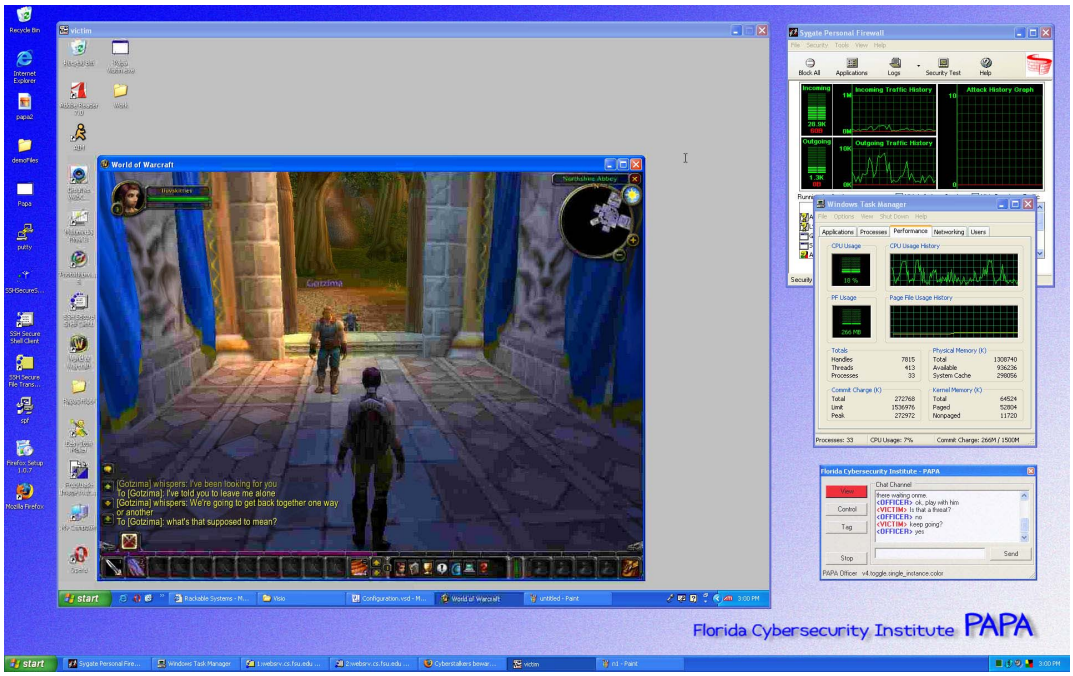

Figure 6. Agent's view of a PAPA session

The Dispatcher Module is a software utility running on a machine expected to be located at a law enforcement site. It monitors the state of the entire system and allows victim and agent to interact over a highly secure channel.

The user interface of PAPA is designed to be extremely simple. Figure 6 shows a screen shot of a victim playing a multi-player network game in which the victim is being harassed. Notice that the chat box indicates that the session is being recorded. The agent and victim are carrying on a text conversation independently of what the victim is doing with the predator.

4.3. Evaluation

Testing of the PAPA system revealed problems that were not initially foreseen. For example, agents found that the chat channel was difficult to use concurrently with taking control of the victim's machine by the agent.

Furthermore, it was difficult to advise the victim through the textual chat channel when at the same time the agent needed to carry on a dialogue with the predator. Similarly, switching from victim control to agent control seemed to be noticeable to the individual acting as the predator.

Additionally, the focus of much of law enforcement activity in this area is in the protection of children where L.E. prefers not to have the minor in the picture at all. This is quite different from the goal of PAPA which was to support adult victims of cyberstalking. Thus L.E. was more inclined to a system where the agent was always in control but could get advice from the victim via an audio channel.

4.4. Privacy and legal aspects

We also explored several legal aspects related to implementing PAPA. For example, the fact that part of the evidence stored is an image of the victim's view on their screen is generally considered as automatically legally permissible.

Storing the full content of IP packets is permissible by the victim under certain conditions, but it appears that storing just the header information might always be allowed without a warrant. Some of these issues are still in a grey area, but may become further clarified as the digital forensics field develops. An operational issue was also important. As cyberstalking of adults is often difficult to classify as a felony, law enforcement is often reluctant to pursue such cases for adult victims; hence the current emphasis on Internet Crimes against Children (ICAC) cases.

4.5. Future work

As the system was built, it became clear that an alternate use was to use the system for training agents in masquerading as children and tracking predators.

There is interest by law enforcement for this training capability for investigating ICAC (Internet crimes against children) cases. This and other similar applications (such as monitoring parolees) would require a somewhat different architecture than was developed.

We are thus planning to build a redesigned version of the PAPA system (PAPA2), with emphasis on training for "meet and greet" sting operations where dialogue with the predator leads to a physical meeting. We focus on making the interactions between the trainer and trainees more convenient to conduct.

5. Conclusion

Creating digital tools for use by law enforcement faces some of the difficulties of other special-purpose software, namely capture of requirements while interacting with non-technical users, in addition to the challenges intrinsic to creating tools that gather court-defensible, forensic-quality evidence. The academic-forensic partnerships at ECIT bring together experts from the technical and law enforcement fields to address these challenges.

6. Acknowledgements

This work was supported in part by the National Institute of Justice under grant 2005-DE-BX-K034 and 2006-DN-BX-K007.

7. References

[1] Sudhir Aggarwal, Daniel Beech, Rajarshi Das, Breno de Medeiros, Eric Thompson, "X-Online: An Online Interface for Digital Decryption Tools," *Proceedings of the 2nd Int. Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE 2007),* April 2007, pp. 105-116

[2] Sudhir Aggarwal, Michael Burmester, Peter Henry, Leo Kermes and Judie Muholland, "Anti-Cyberstalking: The Predator and Prey Alert (PAPA) System," *Proceedings of the 1st Int. Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE 2005)*, November 2005, pp. 195-205.

[3] Sudhir Aggarwal, Peter Henry, Leo Kermes and Judie Muholland, "Evidence Handling in Proactive Cyberstalking Investigations: the PAPA Approach," *Proceedings of the 1st Int. Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE 2005)*, November 2005, pp. 165-176.

[4] Sudhir Aggarwal, Bob Breeden, Peter Henry and Judie Mulholland, "A Training Tool for Internet Crimes Against Children Cases," *in IFIP, Volume 222, Advances in Digital Forensics II*, eds., Olivier, M., Shenoi, S., (Boston, Springer), pp. 317-330, 2006.

[5] Sudhir Aggarwal, Jasbinder Bali, Zhenhai Duan, Leo Kermes, Wayne Liu, Shahank Sahai, and Zhenghui Zhu, "The Design and Development of an Undercover Multipurpose Anti-Spoofing Kit (UnMask)." To appear in *Proc. 23rd Annual Computer Security Applications Conference (ACSAC),* Miami Beach, Florida, December 10-14, 2007.

[6] Casey, E. Practical Approaches to Recovering Encrypted Digital Evidence. *International Journal of Digital Evidence,* vol. 1, no. 3, 2002.

[7] Dunn, J., (2002). Courting disaster: Intimate stalking, culture, and criminal justice. New York: Aldine de Gruyter.

[8] Etter, B. The Forensic Challenges of E-crime. 2001. *Australasian Centre for Policing Research.*

[9] Fisher, R.C. Opinion, on United States vs. Mark S. Forrester and United States vs. Dennis L. Alba. *U.S. Court of Appeals for the 9th Circuit,* 2007.

[10] Law Enforcement Battles with Botnets. *http://government.zdnet.com/?p=2373*, 5/29/07.

[11] Newman, N. and Beathe, M. UnMask Common Practices Report, *National White Collar Crime Center.* November 2006.

[12] Phishing and Federal Law Enforcement. Referenced 5/29/07, http://www.abanet.org/adminlaw/annual2004/Phishing/PhishingABAAug2004Rusch.ppt.

[13] President's Information Technology Advisory Committee (PITAC). Cybersecurity: A Crisis of Prioritization, *Report to the President,* 2/28/2005. http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

[14] Shpantzer, G. and Ipsen, T. Law Enforcement Challenges in Digital Forensics. *Proc. 6th Nat'l Colloquium Information Systems Security Education (CISSE). 2002.*

[15] Wolfe, H. Encountering Encrypted Evidence (potential). In *Proceedings of the Informing Science+ IT Education Conference* (June 19-21), 1601—1607, 2002.

[16] Zona, M., Palarea, R., and Lane, J. The Psychology of Stalking: Clinical and Forensic Perspectives, San Diego, Academic Press, 1998.