Tracking cyberstalkers: a cryptographic approach *

Mike Burmester, Peter Henry, Leo S. Kermes
Department of Computer Science
Florida State University, Tallahassee, FL 32306-4530, USA
Email: {burmester,henry,kermes}@cs.fsu.edu

Abstract

Stalking is a pattern of behavior over time in which a stalker seeks to gain access to, or control over, a victim. Such actions range from the benign to the malicious and may cause emotional distress or harm to the victim. With the widespread adoption of new technologies, new forums of Internet-mediated discourse now exist which offer stalkers unprecedented access to find and exert influence over victims. Cyberstalking, the convergence of stalking and cyberspace, has created new challenges for the prevention, detection, and prosecution of this new phenomenon as the traditional methods of detection by witnesses and enforcement by restraining orders often are inadequate.

In this paper we suggest a cryptographic approach for the tracking of cyberstalkers. We first define the threat model in terms of a profile of the cyberstalker as well as legal and law enforcement constraints. We then describe a monitoring system that addresses the basic security requirements of our threat model by capturing and verifying circumstantial evidence for use in cyberstalking investigations.

Keywords. Cyberstalking, cyberharassment, digital forensics, digital evidence integrity.

1 Introduction

> *Make no mistake: this kind of harassment can be as frightening and as real as being followed and watched in your neighborhood or in your home.*
> Former Vice President Al Gore [31]

The Internet has increasingly become a forum for predator and prey crimes, wherein one party in a relationship seeks to control, exploit, or harm the other by harassment. The harassment can range from unsolicited communication (emails, spam, etc), to repeated, threatening or malicious information. In extreme cases it may extend to luring or enticing victims contacted on the Internet into dangerous physical liaisons.

Cyberstalking generally involves the repeated and persistent attempt by one individual, the stalker, to harass another individual, the victim, using the Internet or more generally an open network. Typically this takes place on networked Personal Computers (PCs), but it can extend to portable devices such as laptops, PDAs (Personal Data Assistants), mobile phones and more generally devices linked to the Internet. Cyberstalking is in many ways analogous to traditional forms of stalking, but by exploiting new technologies and using malicious code (*e.g.*, Trojan code, viruses, time bombs, *etc*), and because of the ubiquity and anonymity provided by the Internet environment, it can take on new forms with unprecedented scope.

Cyberstalking cases present unique challenges for law enforcement [4]. First, the behavior patterns associated with cyberstalking are complex, varied, unpredictable, and difficult to recognize, investigate,

*This material is based on work supported by the NIJ under grant number 2004-RD-CX-K154.

assess and prevent. Some studies indicate that there is no standard predator/prey profile that will universally typify parties [21]. Second, the anonymity provided by the Internet emboldens the perpetrator and complicates the determination of the identity of the stalker [29]. Third, the need to preserve the privacy of legitimate Internet users prohibits direct "wire-tapping" of Internet channels and underscores the need for quality circumstantial evidence.

Law enforcement agents need new tools to address the technical challenges of new technologies, and these emerging types of crime, often perpetrated by resourceful and determined assailants. Ruthless, technologically advanced stalkers can easily intimidate their victims. The social, educational, and economic status of cyberstalkers complicates prosecution in cyberstalking cases. Studies have found that stalkers are generally older than other clinical and offender populations [16, 12, 35]. They are typically better educated than other types of offenders [14], with 22% graduating high school and 6% having graduated college [12]. Frances Grodzinsky and Herman Tavani [10] have noted the ethical issues of cyberstalking in terms of gender, personal privacy, and both virtual and physical harm. Cyberstalkers are typically male and more technically adept than their victims. The online environment makes it relatively easy to maintain anonymity through chat room "avatars", anonymous email accounts, multiple ISPs, and email relay techniques. This anonymity, coupled with the wealth of data available and the ubiquity of the Internet, has frustrated law enforcement, and jurisdictional and statutory limitations often have tied the hands of investigators.

Rapid advances in technology have exacerbated the technical and legal problems facing investigators. The President's Working Group on Unlawful Conduct on the Internet has documented the difficulties of fighting this new form of stalking [30], as law enforcement often lacks the resources to place agents on the scene with the victims, despite efforts to educate victims in best practices for stalking situations [22]. James Moor [17] has pointed to the "policy vacuums" that have arisen because of the new possibilities and "conceptual muddles" caused by the use of networked computers to perpetrate crimes that did not exist in pre-Internet times. Stalking on the Internet leaves an entirely different trail of evidence for investigators that threatens to confound efforts to protect victims. The highly volatile and easily corrupted digital evidence that is often essential for the prosecution, presents new challenges to law makers and forensics experts.

In the past, agents often advised victims simply to stop using the internet, but law enforcement has increasingly adapted traditional techniques for surveillance, investigation, and evidence gathering to networked computer environment [31]. Agents follow the electronic trails left behind by cyberstalkers to discover the patterns of stalking behavior, while preserving the privacy of legitimate users of the network.

In this paper we discuss cyberstalking issues in the general context of a threat model based on a Cryptographic/Steganographic approach and consider possible solutions. We first define (Section 2) our threat model and consider two problems that are closely related to cyberstalking: the Prisoner's problem and the Man-in-the-Middle problem. Then (Section 3) we propose a "blackbox" monitoring system that will track the actions of cyberstalkers as a general forensics tool that will address the security issues of our cyberstalker threat model. We conclude (Section 4) with a discussion of implementation issues.

2 A cyberstalking threat model: the Cyberstalker's profile, Law Enforcement constraints and the Cyberstalker's problem

Our threat model has three basic components: the Cyberstalker's profile, the Law Enforcement constraints and the Cyberstalker's problem.

2.1 The Cyberstalker's profile

Cyberstalking, and more generally cyberharassment, are characterized by the stalker's relentless pursuit of the victim online and are likely to include or evolve into some form of offline attack. Cyberstalkers can be known or unknown to their victim and are often driven by revenge, hate, anger, jealousy, obsession and mental illness, while cyberharassers are often driven by the desire to frighten or embarrass the victim [33]. The harassment may take several forms, including:

1. Posting comments intended to cause distress to the victim and/or make them subject of harassment by others.
2. Sending a stream of unsolicited messages (possibly hateful or provocative) to the victim or to associates of the victim.
3. Sending or posting offensive or hateful comments or lies in their own identity or impersonating the victim.
4. Hacking or taking over the victim's computer or email accounts.
5. Changing the victim's password and blocking their account.
6. Signing the victim up for spam, porn sites or questionable offers.
7. Following the victim into cyber chat rooms or discussion boards.
8. Creating sexually explicit images of the victim and/or posting them on Web sites, or commercial porn sites.
9. Luring, or enticing, the victim into an offline meeting.

The last form of harassment is perhaps the most dangerous because of the potential to lead to direct physical harm. The wide variety of stalking and harassing enabled by the increasing power and reach of networked computers and evolving technologies has made it possible to deliver content anonymously. This is exacerbated by the technical proficiency of stalkers, which often exceeds the capability of the victims and the law enforcement agents. We propose a monitor system that is able to captures data only from the PC of the victim, without resorting to internet techniques. Although it cannot directly combat all the categories above, it can effectively document and verify: (i) messages sent directly to the victim, (ii) attempts to hijack the victim's computer, (iii) cyberstalking in chat rooms and discussion boards and, (iv) sexually explicit messages sent to the victim directly.

2.2 Law enforcement constraints – consent, digital evidence integrity, chain-of-custody

The Monitor system that we propose is intrusive to the victim because it requires the insertion of both hardware and software into the victim's computer environment that are capable of capturing private and sensitive communication between the victim (and other users, if the computer is a multi-user platform) and legitimate parties. Additionally, there may be confidential files on the computer that the victims does not want the investigator to see. These concerns must be addressed on a case by case basis. Strategies include giving the victim a dedicated computer to use during the investigation, quarantining existing files, making Monitor sessions specific only to the victim, and demanding consent from the victim at the beginning of each session through an authorization dialog.

As we have seen, victims of cyberstalking are often isolated, intimidated, and technologically unable to effectively respond to the threat. In addition, the collection of quality evidence in cybercrime is problematic. Even when law enforcement agents are directly involved in investigating cybercrime, great care

must be taken in the collection, recording, and verification of digital evidence. Evidence in a criminal court is authenticated through standardized evidence handling procedures and chain-of-custody records that have traditionally relied on physical security measures. Digital evidence offers new challenges for authentication because it is so easily copied, deleted, and modified. Erik Berg [2] has argued that digital images may require that special care be given to document the collection and analysis procedures and the chain-of-custody to ensure admissibility. Thomas Duerr *et al* [7] agree that digital evidence is potentially more susceptible to post-collection alteration than analog evidence, but argue that there are information assurance methods developed for Internet applications and electronic commerce that can enhance current evidence handling and chain-of-custody documentation procedures for their integrity. The Information Assurance Technical Framework [20] delineates five primary security services relevant to information and information processing systems: access control, confidentiality, integrity, availability, and non-repudiation. Confidentiality and availability are not directly concerned with the authentication of digital evidence, but integrity is essential. Duerr *et al* [7] argue that "it is desirable to ensure the integrity of the data as close to the source format and as near to the time and place of collection as feasible", and that "identification of the user who collects the evidence and generates the integrity data should be integral to the solution." They stress that the integrity process must not be allowed to modify the original data in any way. Non-repudiation and access control services are also necessary to bolster chain-of-custody record keeping and to maintain an audit trail of successful and unsuccessful access attempts (it is essential to prove *who* handled a piece of evidence and *when*). Because methods of digital evidence integrity verification are often new and have not yet been used in criminal courts, they may be subject to a Daubert challenge [5] that requires the judge to assess the validity and applicability to the case of the technique or methodology invoked by expert testimony. The Daubert ruling provides aids for the judge in making that assessment. These are based on the reliability and general acceptance in the scientific community of the techniques or methodologies used. In particular, authentication systems must strictly adhere to existing government and industry standards and accepted practices set forward by the National Institute for Standards and Technology (NIST) for government and commercial cryptographic algorithms and equipment.

2.3 The Cyberstalker's problem, the man-in-the-middle problem and the Prisoner's problem

The *Cyberstalker's problem* is a three party communication game involving *a Victim* (Alice), *the Stalker* (Bob) and *a Monitor* – see Figure 1. Bob and Alice are linked by a communication channel which can be accessed by the Monitor. The goal of Bob is to harass Alice while the goal of the Monitor is to record any such activity. In the traditional cryptographic terminology, Bob wants to establish a (virtual) *harassment* channel, while the Monitor wants to track it and record its content.

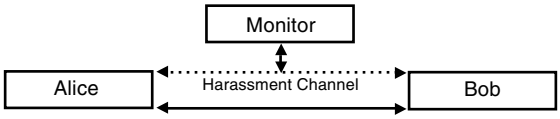

Figure 1: The Cyberstalker's problem: the Monitor has to capture harassment data exchanged by Alice and Bob.

This problem is related to the classical Prisoner's problem [24] in Steganography (Information Hiding) which also involves three parties. In this case, Bob is incarcerated, Alice is free and the Monitor (Wendy) is a Warden – see Figure 2. Alice has hatched out an escape plan and visits Bob with the intention of passing on details of her plan. Any exchange of information must take place in the presence of Wendy. To succeed, Alice must hide her escape plan in what appears to be innocuous information.

If Wendy detects that secret information is hidden in their communication then the Bob's escape will be thwarted. The channel that Alice and Bob want to establish is called a *subliminal* (or *covert*) channel.

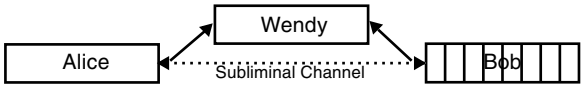

Figure 2: The Prisoners's problem: Wendy has to prevent Alice from sending Bob a covert message.

The man-in-the-middle problem [1, 25, 8] is a similar problem that has been extensively studied in Cryptography. In this case the Monitor is the adversary (Eve) – see Figure 3. Eve may be *passive* and simply eavesdrop on the communication between Alice and Bob, and/or *active*. An active adversary can corrupt messages sent to Bob (or Alice) by Alice (Bob) or impersonate one party to the other.

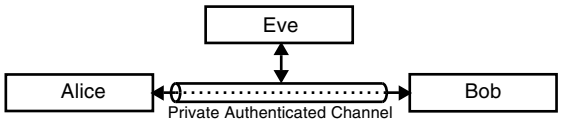

Figure 3: The man-in-the-middle problem: Alice and Bob have to establish a private and/or authenticated communication channel in the presence of Eve.

The last two problems are fundamental to Steganography and Cryptography, and define their respective threat models. Dealing with them has been the focus of research in these disciplines (see *e.g.*, [24, 3, 34, 1, 25, 8]). What characterizes all three problems is their adversarial nature. In the Cyberstalker's problem the Stalker is the adversary and the other two collaborate to detect and record any harassment. In the Prisoner's problem, Alice and Bob conspire to establish a subliminal channel. For this problem, *they* are the adversary. The Warden's goal is to make sure that their communication channel is *subliminal-free*. In the man-in-the-middle problem, Eve is the adversary. Eve's task is to undermine the privacy and/or authenticity of the communication between Alice and Bob. Alice and Bob want to establish a private and/or authentication channel to secure their communication.

The Cyberstalker's problem focuses on *capturing* harassment data rather than direct *prevention* of harassment, while the other two problems focus on prevention. This makes it easier in some respects to deal with cyberstalking – at least from a cryptographic point of view. The main difficulties are the forensics aspects of (i) the data capturing process and (ii) the verification of the captured data. Security is based on the data's evidentiary value. The Cyberstalker's problem describes in general terms the cyberstalking threat model, and we will use it as our basic security model.

2.4 The cyberstalking security model

We consider two oracles: an oracle for the cyberstalker's profile $\mathcal{O}_{harass}$, and an oracle for the law enforcement constraints $\mathcal{O}_{law}$. Given any data, $\mathcal{O}_{harass}$ rules whether the data is (bit 1), or is not (bit 0) listed in the cyberstalker's harassment profile. Given the capturing process and the captured data of a monitor M, $\mathcal{O}_{law}$ rules whether this satisfies (bit 1), or does not (bit 0), the law enforcements constraints regarding the victim's consent, the digital evidence integrity and chain-of-custody.

We say that the monitor M is a *secure solution* of the Cyberstalker's problem if, for all $data_{Alice,Bob}$ that Bob and Alice exchange,

$$\mathcal{O}_{harass}(data_{Alice,Bob}) = 1 \text{ implies } \mathcal{O}_{law}(M_{Alice,Bob}(data_{Alice,Bob})) = 1.$$

That is, a secure solution to the Cyberstalker's problem is a monitor M that captures all data in the harassment list in a lawful way.

3 A Cyberstalker Monitor system

In the previous section we defined our threat model. We now consider secure solutions. These will be based on a monitoring system that captures harassment data in such a way that both the capturing process and the data will be admissible evidence in a criminal court.

Our proposed Monitor is a tool meant to complement traditional forensics tools. It may not directly identify the stalker, but will allow investigators to uncover patterns of behavior, trails to computers that the stalker may have used, and other potentially relevant forensic data that would have been discarded otherwise.

3.1 A first approach: a low-tech analog solution

An obvious solution is to have a law enforcement agent alongside the victim to monitor cyberstalking sessions. A more practical solution is to replace the agent by a closed-circuit television camera and a recorder to monitor the sessions – see Figure 4. Both of these solutions will provide evidence of stalking,

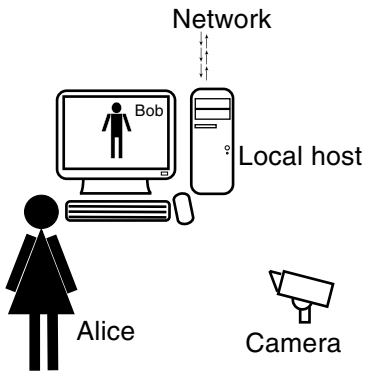

Figure 4: A low-tech solution: harassment data is captured on a closed-circuit television camera.

but offer only a weak binding of the stalker to the session. Evidence from the actual TCP/IP packets received could help strengthen the link.

3.2 A basic Cyberstalker Monitor system

In this system a blackbox Monitor is used to capture the local host data and the relevant network data – see Figure 5. The local host data includes data on the PC of the victim: the contents of the screen buffer,

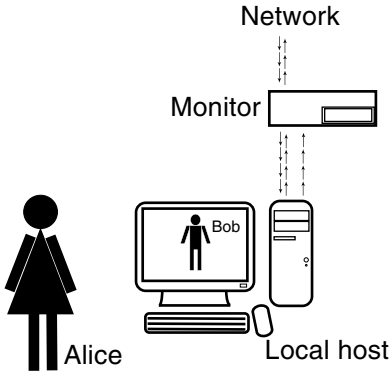

Figure 5: The Cyberstalker Monitor System captures and stores local host data and network data.

audio buffer, keystrokes and mouse data. The relevant network data includes all the incoming/outgoing network packets, excluding machine generated overhead. Data is captured and stored locally in the Monitor (on a hard drive).

The Monitor contains a transparent network bridge with connections to the network (Internet) and the local host (the Victim's PC) and a storage device – see Figure 6. The storage device has two modules.

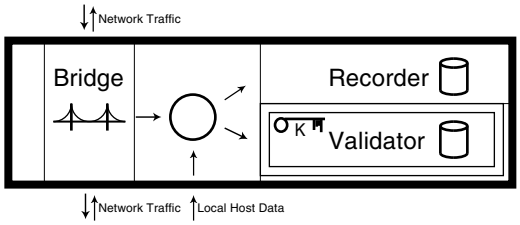

Figure 6: The Monitor has a transparent network bridge, a Recorder and a Validator.

A Recorder that captures local host data and network data and a physically secure Validator that stores evidence integrity data and a cryptographic key (K).

The Monitor operates on the concept of a session. A session is initiated upon the victim's connection to the network and lasts until disconnection. During the session, the local host data is stored on the Recorder and authenticated using a keyed hash function HMAK [13] with hash function SHA-1 [19]. This produces a digest which is the evidence integrity data. A symmetric key is used that is stored in a secured (tamper-resistant) region of the Validator (and cannot be extracted). A duplicate key is kept in the forensics lab of the law enforcement agency. To validate captured data for use as evidence in court, the data and its integrity validator are extracted and the duplicate key is used to validate the data. The cryptographic details of the process of validation of the integrity of the evidence data are as follows. Let

$data_{session(sn)} = (cn, sn, T_{lh}, T_{mon}, \{data_{lh}, data_{mon}\}, T^*_{lh}, T^*_{mon})$

be the data with case number cn, session number sn, start timestamps T_{lh}, T_{mon}, end timestamps T^*_{lh}, T^*_{mon}, for the local host and Monitor respectively, and session stream data $\{data_{lh}, data_{mon}\}$, formatted in such a way that it can be hashed as a stream,[1] and let

$\mathrm{HMAC}_{K_{cn}}^{\mathrm{SHA}}(data_{session(sn)})$

be its HMAC digest with hash function SHA-1 and key K_{cn}.[2] The data integrity validator is,

$integrity\_validator_{session(sn)} = (cn, sn, \mathrm{HMAC}_{K_{cn}}^{\mathrm{SHA}}(data_{session(sn)}))$.

To validate extracted data, the duplicate key is used to compute its keyed digest and the result compared with the integrity validator for that session. If the values agree, then the data has not been corrupted.

Observe that it might be tempting to send the integrity validation data (the digest) through the existing network directly to the forensics lab for secure storage, but this should be avoided because it violates the transparency of the bridge, making it possible for the stalker to detect the presence of the Monitor. The separation of the functions of the Monitor and of the local host is a crucial security requirement [6].

3.3 Securing the Cyberstalking Monitor

We can replace the symmetric key used in the Cyberstalker Monitor with an asymmetric key, *e.g.*, a DSS key [19]. In this case a private key SK_{cn} is stored in the Validator module and the corresponding public key PK_{cn} is stored in the forensics lab – see Figure 7. This strengthens the evidentiary value of the captured data and extends the chain-of-custody (secrecy is not needed for the public key PK_{cn}), but does not offer any other significant advantage.

[1] Bits from $data_{lh}$ are interleaved with bits from $data_{mon}$.

[2] $\mathrm{HMAC}_{K_{cn}}^{\mathrm{SHA}}(data) = \mathrm{SHA}(K_{cn} \text{ XOR } opad, \mathrm{SHA}(K_{cn} \text{ XOR } ipad, data))$, where $opad$ and $ipad$ are appropriate outer and inner paddings. A different key K_{cn} is used for each case cn.

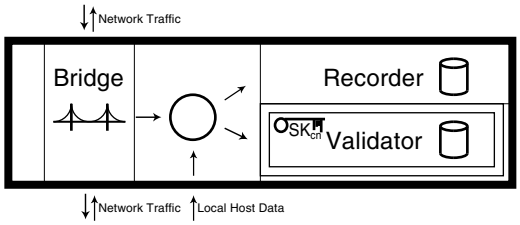

Figure 7: The Monitor with an asymmetric key.

A significant security advantage is achieved by separating the duties of the Recorder and Validator.[3] For this purpose, we may use an independent communication channel (one that is not associated with the Victim in any way) to send the evidence integrity validation (the digest) to the forensics lab, where it is securely logged. For practical purposes we may use wireless communication technology to broadcast securely to a network controlled by the law enforcement agency. Figure 8 illustrates an application which uses wireless technologies.

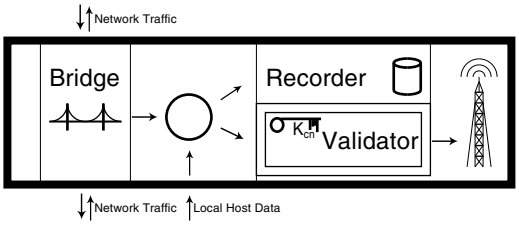

Figure 8: The Monitor with a wireless device.

The independent communication channel could also enable additional functionality to make the system more flexible. First, with a high bandwidth channel, Virtual Network Computing (VNC) could be used to allow the investigator to remotely monitor and control the Victim's desktop. Second, session "reports" containing important system information (remaining disk space, amount of data recorded, etc.) could be sent to the investigator. Third, reports could include snapshots (screen images) of significant events tagged by the victim. Finally this channel can be used to synchronize the clock of the Monitor to the clock of the forensics lab. All of these enhancements would help the investigator monitor more closely the case and respond in person if required.

The physical tamper-resistance of the Monitor can be supported by case-intrusion detection mechanisms and real-time notification of tampering or system failure through a "heartbeat" mechanism.[4] For fine granularity, a heartbeat signal from the internal clock of the Monitor is recorded on the Validator disk (on a cyclic log). For course granularity, at regular intervals (*e.g.*, once a day), the heartbeat is broadcast to the forensics lab.

3.4 Policies concerning the Cyberstalking Monitor

Because of the intrusiveness of the Monitor, policies must be written for the deployment/retraction, key management, extraction and storage of data, to follow all applicable laws, preserve the integrity of the evidence and chain-of-custody. Detailed discussion of policy considerations is dependent on jurisdictional considerations as well as privacy considerations for the innocent, and go beyond the scope of this paper.

[3] Separation of duties is a fundamental requirement for Trusted System security [6].

[4] A heartbeat is a signal that is emitted at regular intervals by software to demonstrate that it is still alive. Sometimes hardware is designed to react if it stops hearing a heartbeat.

3.5 A security proof

In Section 2.4 we proposed a security model for cyberstalking. We shall use this model to prove that our Monitor is a secure solution for the cyberstalker's problem. Suppose that $\mathcal{O}_{harass}(data) = 1$ for some captured data, that is, $data$ is in the harassment list. We have to show that $\mathcal{O}_{law}M(data) = 1$, that is that, M has captured this data in a lawful way. This follows from the fact that:

- the Monitor is tamper-resistant,
- the Monitor is transparant,
- we have separation of duties,
- the data is validated using acceptable practices and standards, and
- applicable laws and policies regarding chain-of-custody are followed.

4 Implementation

4.1 Hardware

Implementation of the Monitor can be achieved though the use of commodity hardware. The following considerations should be made in selecting such hardware.

1. As far as possible, industry standard security components for environments that involve trust, security, and reliability should be used.
2. The power consumption should be low.
3. The footprint of the device should be minimal (to lessen consumption of the victim's space).
4. Annoyances such as heat and noise should be avoided (noise may affect the victim's willingness to use the device in his or her environment.
5. The hardware should be able to perform the required tasks reliably.

4.2 Software

The Monitor must have an operating system, and we recommend the use of any one of the many hardened Linux Distributions of the NSA's SE Linux project for security, hardware compatibility, and developer community oversight. These operating systems have robust journaling file systems as well as secure access control mechanisms.

Several pieces of software must be developed for our system. Depending on the OS of the Victim's local host, either a system service (Microsoft Windows) or a daemon process (Linux) must be written to gather the local host data in real time and send it to the Monitor. On the Monitor, we must write a daemon for each one of its modules as well as an application for configuring the Monitor. Also, a suite of applications must be developed for the extraction, verification and analysis of the data collected by the Monitor. NIST standards should be used in the implementation of our system and the best software engineering practices adopted, so that the implementation can benefit from the scrutiny of public review.

4.3 User interaction

From a software engineer's point of view, the Monitor system has three users: the Victim, a Law Enforcement Officer, and a Forensics Lab Technician.

- For the Victim, the Monitor is transparent and has no effect on the normal use of the local host with the exception of a splash screen and system tray icon that notifies the user that the Monitor is active.
- For the Law Enforcement, Officer the Monitor is an appliance: simple connections (USB and Network Bridge) are made when the Monitor is first installed.
- For the Forensics Lab Technician, the Monitor is a Linux system. To set up the Monitor for deployment, the Technician attaches a display, keyboard and mouse and logs into the local console of the Monitor to configure the system and load the case number and encryption key. On return from deployment, the Technician unlocks the Monitor, ejects the disk and loads it on another system for the extraction, verification and analysis of the data. The disc is stored securely as digital evidence and investigators work off of verified copies.

Acknowledgements

The authors would like thank all those who have helped this project: Judie Mulholland, Sudhir Aggarwal, Breno de Madeiros, Alec Yasinsac, and Tri Le-Van.

References

[1] S. Bengio, G. Brassard, Y.G. Desmedt, C. Goutier, J.-J.Quisquater. *Secure implementations of identification systems*. J. Cryptol. **4**(3) (1991) 171–183.

[2] E.C. Berg. *Legal ramifications of digital imaging in law enforcement*. Forensic Science Communications [Online], October 2000. Available from: www.fbi.gov/hq/lab/fsc/backissu/oct2000/berg.htm.

[3] M. Burmester, Y. Desmedt, T. Itoh, H. Shizuya, M. Yung. *A progress report on subliminal-free channels*. Information Hiding, First International Workshop, Cambridge, Lecture Notes in Computer Science No. 1174, Springer, Berlin, 1996, pp. 151–168.

[4] M. DÁmico. *The Law vs. Online Stalking*, February Online FAQ, 1997. Available from: http://www.madcapps.com/writings/faqabout.htm.

[5] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 US, 579 (1993).

[6] Department of Defense. *Trusted Computer System Evaluation Criteria (TCSEC), also known as Orange Book*. December 1985. Available from: http://www.radium.ncsc.mil/tpep/library/rainbow/5200.28-STD.html

[7] T.D. Duerr, N.D. Beser and G.P. Staisiunas. (2004). *Information Assurance Applied to Authentication of Digital Evidence. Forensic Science Communications.* **6**(4), October, 2004. Available from: http://www.fbi.gov/hq/lab/fsc/backissu/oct2004/research/2004_10_research01.htm.

[8] Ferguson, N., & B. Schneier. *Practical Cryptography*. Wiley Publishing Inc., Indianapolis, 2003.

[9] T. Gregorie. *Cyberstalking: Dangers on the Information Superhighway*, 2002. Available from: http://www.ncvc.org/src/help/cyberstalking.html.

[10] F. Grodzinsky and H. Tavani. *Cyberstalking, Moral Responsibility, and Legal Liability Issues for Internet Service Providers*. In Josep Herkert, ed. *Proceedings of ISTAS 2002: The International Symposium on Technology and Society*, Los Almito, CA, IEEE Computer Society Press. 331-339, 2002.

[11] S. Hardman. *Stalking: Impact, Law, Sentencing and Stalking On-Line*. Forensic Criminology Services, 2003. Available from: http://www.forensic-crim.com/readings/stalking.htm.

[12] R.B. Harmon, R. Rosner and H. Owens. *Obsessional harassment and erotomania in a criminal court population.* Journal of Forensic Sciences, 40, 2, 188 - 196, 1995.

[13] H. Krawczyk, M. Bellare and R.Canetti. *HMAC: Keyed-Hashing for Message Authentication.* RCF 2104 (RFC 2104), Internet RCF/STD/FYI/BCP Archives, 1997. Available from: http://www.faqs.org/rfcs/rfc2104.html

[14] R. Lloyd-Goldstein. *DéClerembault On-Line: A Survey of Eratomania and Stalking from the Old World to the Worl Wide Web*. In J.R. Meloy, *The Psychology of Stalking: Clinical and Forensic Perspectives*, San Diego, Academic Press, 1998.

[15] J.R. Meloy. *Stalking (obsessional following): A review of Some Preliminary Studies*. Aggression and Violent Behaviour, 1 (2), 147 - 162, 1996.

[16] J.R. Meloy. *Unrequited Love and the Wish to kill: Diagnosis and Treatment of Borderline Eratomania*. The Bulletin of the Meninger Clinic, **53**, pp. 477–492, 1989.

[17] J. Moor. *Reason, Relativity, and Responsibility in Computer Ethics*. Computers and Society, Vol. 28, No. 1, pp. 14-21, 1998.

[18] National Institute for Standards and Technology (NIST). *FIPS 180-2, Secure Hash Standard (SHS)*, August 2002. Available from:
http://csrc.nist.gov/CryptoToolkit/tkhash.html

[19] National Institute for Standards and Technology (NIST). *FIPS FIPS 186-2, Digital Signature Standard (DSS)*, February 2000. Available from: http://csrc.nist.gov/CryptoToolkit/tkdigsigs.html

[20] *National Security Agency Information Assurance Solutions Technical Directors. Information Assurance Technical Framework*. Release 3.1, September 2002. Available from: http://www.iatf.net/framework_docs/version-3_1/index.cfm.

[21] W. Petherick. *Cyber-stalking: Obsessional Pursuit And The Digital Criminal*, 2003. Available from: http://www.crimelibrary.com/criminology/cyberstalking/.

[22] B. Ramsey. *Stop the Stalker: A Guide for Targets*, Securus House, 2000.

[23] T. Richardson. *The RFB Protocol*, 2004. Available from:
http://www.realvnc.com/docs/rfbproto.pdf.

[24] G.J. Simmons. *The Prisoner Problem and the Subliminal Channel*. Proceedings of CRYPTO'83, Plenum Press, pp. 51–67, 1984.

[25] B. Schneier, *Applied Cryptography*, 2nd Edition John Wiley & Sons, 1996.

[26] *Stalking Victimization*. OVC Pamphlet, posted. Available from:
http://www.ojp.usdoj.gov/ovc/publications/infores/help_series/pdftxt/stalkingvictimization.pdf.

[27] *The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet*, a Report prepared for the President's Working Group on Unlawful Conduct on the Internet. Available from: http://www.usdoj.gov/criminal/cybercrime/unlawful.htm.

[28] US Department of Justice. *Stalking Victimization*, OVC Pamphlet, 2004. Available from: http://www.ojp.usdoj.gov/ovc/publications/infores/help_series/pdftxt/stalkingvictimization.pdf.

[29] US Department of Justice. *Stalking and Domestic Violence: Report to Congress*. Report from the Attorney General to the Vice President, 2001. Available from: http://www.ncjrs.org/pdffiles1/ojp/186157.pdf.

[30] US Department of Justice. *The Electronic Frontier: the Challenge of Unlawful Conduct Involving the Use of the Internet*. Report prepared for the President's Working Group on Unlawful Conduct on the Internet, 2000. Available from: http://www.usdoj.gov/criminal/cybercrime/unlawful.htm.

[31] US Department of Justice. *Cyberstalking: A New Challenge for Law Enforcement and Industry. A Report from the Attorney General to the Vice President*, August 1999. Available from: http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm.

[32] G. Wattendorf. *Stalking Investigation Strategies*. FBI Law Enforcement Bulletin, pp. 10-14, March 2000.

[33] Wired Patrol, *Internet safety, Help and Education*, 2004 Available from: http://www.iredpatrol.org/cyberstalking_harassment/.

[34] A. Young and M. Yung. *Malicious Cryptography: Exposing Cryptovirology*. John Wiley & Sons, 2004.

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