Embedding Hercule Poirot in Networks: Addressing Inefficiencies in Digital Forensic Investigations

Barbara Endicott-Popovsky[1] and Deborah A. Frincke[2]

[1] University of Washington
[2] Pacific Northwest National Labs
endicott@u.washington.edu, deborah.frincke@pnl.gov

Abstract. Forensic investigations on networks are not scalable in terms of time and money [1]. Those investigations that do occur consume months of attention from the very experts who should be investing in more productive activities, like designing and improving network performance [1]. Given these circumstances, organizations often must select which cases to pursue, ignoring many that could be prosecuted, if time allowed. Recognizing the exponential growth in the number of crimes that employ computers and networks that become subject to digital evidence procedures, researchers and practitioners, alike, have called for embedding forensics—essentially integrating the cognitive skills of a detective into the network [2, 3, 4]. The premise is that the level of effort required to document incidents can thus be reduced, significantly. This paper introduces what technical factors might reflect those detecting skills, leading to solutions that could offset the inefficiencies of current practice.

Keywords: Network forensics, digital forensics, computer crime, augmented cognition.

1 Introduction to the Problem

Unlike most crime scenes where crime tape isolates the scene allowing experienced forensic investigators the luxury of time to gather admissible evidence, a digital crime scene is an active network with the network administrators functioning as first responders. Often they are unaware of courtroom evidence gathering requirements [1, 3]. Practitioners who do consider collecting network forensic data face a choice between expending extraordinary effort (time and money) collecting forensically sound data, or simply restoring the network as quickly as possible. They most often make the expedient choice—responding to distraught users by restoring network function immediately, ignoring the rigors of collecting and preserving forensically sound data [3]. This translates to key evidentiary files most likely altered in the process, limiting their value in the courtroom and opening them to legal challenge [5].

This paper explores this problem and the forces for change that will require rethinking network design to include embedded forensics that substitute for the crime

D.D. Schmorrow, L.M. Reeves (Eds.): Augmented Cognition, HCII 2007, LNAI 4565, pp. 364–372, 2007.

scene detective. We believe the methods of augmented cognition can offer insight into this transformation and initiate exploration of this idea in the context of our existing research.

1.1 Motivation for Change

In today's world, digital evidence gathered hastily, without regard to its admissibility, may be admitted anyway, with law enforcement and legal professionals often unaware of the potential legal problems that could arise [5]. A review of several hundred pages of computer forensic testimony in cases from 2000 to present, confirmed this concern [6]. Technical competence ranged from minimal to highly professional, reflecting the state of the legal system with regard to digital forensics. Not only are those responding to a crime scene unprepared, the fact that there are no agreed-upon professional standards for network forensic procedures means the court system and legal professionals are likewise unprepared.

While legal arguments on both sides of the bar—defense and prosecution—have been technically unsophisticated to date, it is not expected that the *status quo* will remain. Several trends are motivating change.

To identify a few:

1) The threat spectrum is growing and indicates a movement toward organized crime as the predominant beneficiary of online criminal activities [7]. This means more online crime and bigger losses. As an example, estimates of the impacts to the world economy indicate that the dollar amount of online theft exceeds the profits of e-commerce by almost two to one [8].
2) In light of recent legislation, legal counsel, in the interest of establishing evidence of due care, have begun urging organizations to invest in procedures and technology that will allow collection of forensically sound data defensible in a court of law [9]. This is precipitating efforts by organizations such as NIST and IFIP to converge on digital forensics standards that can be relied upon in the courtroom. [10]
3) As a result, organizations face an urgent need to 're-think' incident response and the role of digital forensics among their network strategies if they wish to deter the growing threat by pursuing, and assisting in the capture of, online criminals. [11]

1.2 Examining Two Criminal Cases

In [1] the authors explored two successfully prosecuted computer crimes that demonstrate the need for a preventive and proactive response to malicious intrusion. The comparison indicates the growing costs and consequences of professional criminals beginning to dominate online crime, as well as the challenge of finding experts to execute forensic investigations. The findings are summarized in Table 1.

Table 1. Criminal Case Comparison

Characteristics	*Script Kiddy*[1] *Case*	*Professional Criminal Case*
Type of attack	Exploitation of a network vulnerability to perform a denial of service attack	Online automated auction scam
Damages	$400,000	$25 million
Investigator time	417 hours	9 months
Investigation costs	$27,800	$100,000 (partial)
Consequences	Community service	3 & 4 years in prison
Investigator	Sys admins learning forensics	Expert recruited by the FBI
Forensic readiness	Reactive	Reactive.

Analysis of the results suggests that the investigations required to successfully prosecute these cases, are not scalable. The costs per incident are too high, take too much organizational time and result in comparatively little consequence to the offender. The study further concluded that there is a need to "operationalize" the concept of organizational network forensic readiness, defined as 'maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response' [2]. This is essentially the act of 'embedding a detective' in networks--capturing the expertise of the crime scene investigator, including the procedures needed to collect admissible evidence, in lieu of *ad hoc* investigations by non-law enforcement.

Without relying on training network administrators to become law enforcement professionals, this means rethinking strategies for protecting networked systems and ultimately redesigning them to include the characteristics of good detection.

1.3 Changing Strategies

In [11], the authors proposed a strategic framework (Table 2), derived from Carnegie Mellon's 3R model for survivable systems, as a vehicle for rethinking network protection strategies [12]. By the addition of a 4th R–*Redress*—defined as the ability to hold intruders accountable—the focus of network protection changes from purely defensive to include offensive strategies. A 4R approach changes the desired outcome of an attack from "patch and recover" to include identification of the attacker. As a consequence, it also expands the duties of those responsible for securing networks to include employing the skills of a detective at a crime scene [11].

Implementing a 4R strategy in an organization will necessitate re-examination of current security policies, procedures, methods, mechanisms, and tools in order to ensure compliance with courtroom admissibility standards and to include the requirements of a skilled detective. This implies a need for a comprehensive approach for incorporating digital forensic investigation into networked systems.

[1] A script kiddy is a recreational hacker with little skill who uses readily available, already-developed hacking tools for online mischief.

Table 2. 4R Strategies for defendingforensically ready networks

Strategy	*Tools*
Resistance Ability to repel attacks	• Firewalls • User authentication • Diversification
Recognition 1) Ability to detect an attack or a probe 2) Ability to react / adapt during an attack	• Intrusion detection systems • Internal integrity checks
Recovery 1) Provide essential services during attack 2) Restore services following an attack	• Incident response • ("forensics" - *the what)* • Replication • Backup systems • Fault tolerant designs
Redress 1) Ability to hold intruders accountable 2) Ability to retaliate	• Forensics - *the who* • Legal remedies • Active defense

1.4 The Research Gap

As early as 2001, researchers participating in the annual *Digital Forensics Research Workshops* (*http://www.dfrws.org/*) identified the lack of a conceptual framework for proactive approaches to digital forensics from the 'organization-as-first-responder' viewpoint. Instead the primary research focus has been on forensic methods, tools and techniques, largely from a law enforcement perspective [13]. Table 3 summarizes the distribution of DFRWS research from 2002 to 2006:

Table 3. Distribution of presentations DFRWS 2002-2006

Research Category	**Number of Presentations**
Education	2
Evidence analysis and management	16
File system forensics	3
Investigation	6
Network forensics	13
Standards and methods	12
Comprehensive framework	1
Tools	7

As one of the premiere venues for digital forensics research, the DFRWS is indicative of the research emphasis in the field of digital forensics to date. The gap identified in 2001—the lack of a conceptual framework for digital forensics—has not yet been resolved, particularly from a user's perspective [14].

2 Life Cycle Methodology

To begin to address this gap, in [1] we proposed an implementation framework—the life cycle methodology shown in Fig. 1. The NFDLC (Network Forensics Development Life Cycle) describes, from an organization view, how the skills of a detective can be embedded in systems. The methodology is based on the NIST Information Systems Development Life Cycle (ISDLC) that incorporates security across the life cycle [15] and is integrated with detection skill requirements, including compliance with legal considerations, such as evidence admissibility rules.

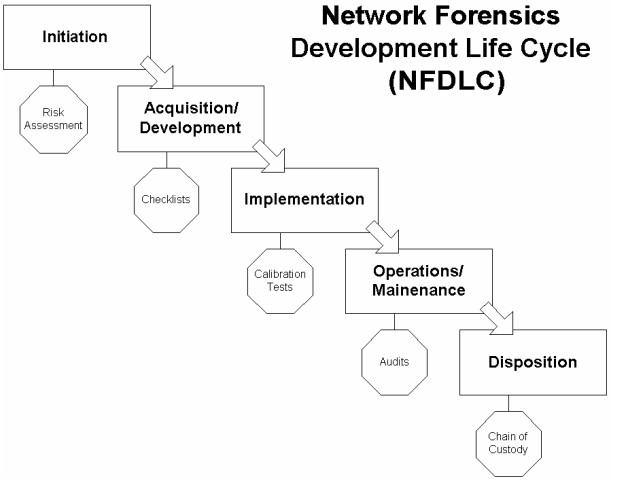

Fig. 1. Modifications to the ISDLC to embed digital forensics

As a result, the following changes to the ISDLC were recommended [14]:

Initiation phase: The risk assessment task would expand to include a determination of what aspects of a network would warrant digital forensic protection. Discussions with practitioners led to the conclusion that not all elements of a network would warrant the investment in embedded forensics [16]. Determination of where forensic investments should be made would involve an analysis of legal risk and liability.

Acquisition/Development phase: Checklists, like those developed by other researchers [4, 17-19], would be appropriate to determine what forensic procedures/tools/ technologies should be embedded in the network. In many instances, these will require modification to include the skills of a detective. An example from our current research will be discussed subsequently.

Implementation phase: Calibration testing would be added. Today's manufacturers of network devices may provide general specifications, but few guarantee actual device behavior. The consequences of failing to validate behavior could lead to inadmissible evidence through legal challenge and failed legal action. Calibration can provide the needed validation of device reliability and predictability [5].

Operation/Maintenance phase: Calibration audits would be added to confirm results of previous calibration tests because as the network grows and changes, re-testing will be necessary.

Disposition phase: Chain of custody procedures would be incorporated to ensure preservation of potential evidence residing in retired systems.

3 Progress to Date

Detailed content of the NFDLC methodology is under development. We began with calibration testing in the Implementation phase because we saw an immediate need. Existing network devices, such as switches and taps with span port capability, are used already to collect network traffic data for the courtroom. If they are not calibrated, expert testimony can be compromised as described in [5].

A generalized framework for developing calibration tests, the OCTDF (Fig. 2), evolved from tests devised for a specific forensic tap [5]. This has spawned an avenue of inquiry that we continue to pursue as we scale the OCTDF to more complex network devices and in different application contexts [20].

Observability Calibration Test Development Framework (OCTDF)

1) *Step 1*: Identify Potential Challenge Areas and Environment
Identification is accomplished by briefly modeling interactions of interest given a particular scenario; then using that information to identify whether, or not, lost network data could damage evidence value. The result will be a set of pairs of behavior to be observed, and the circumstances under which that observation is expected to take place.

2) *Step 2*: Identify Calibration Testing Goals
Given each pairing of behaviors to be observed, and the likely circumstance for observation, testing goals are identified that are supportive of demonstrating evidence value.

3) *Step 3*: Devise a Test Protocol.
From the testing goals identified in Step 2, a testing protocol is devised that will provide appropriate calibration for the device in question.

Fig. 2. Framework for calibration test protocols

Our attention has turned to development of the remainder of the methodology, which we've anthropomorphized through the metaphor of 'embedding a detective in the network.' The network becomes the detective. While network data is being collected today at various nodes, its use as evidence is incidental to its prime function—network management. We contend existing network tools will require modification to include detection considerations. An example would be intrusion detection systems (IDS) that today alert network administrators to possible incursions.

Intrusion detection systems (IDS) were designed to augment cognition of network administrators managing security on networks. They provide alerts that a possible intrusion has occurred. They are tuned to either signatures of known intrusion scenarios or anomalous behavior and are designed primarily to provide data for human decision-making. The data comes from a variety of sources—i.e., audit log, systems logs, host OS—originally designed to assist with administering systems, but never intended to be employed as evidence-gathering devices for the courtroom.

If IDS systems were to assume the role of embedded detective, complete with an understanding of admissibility requirements, they would need to be modified to reflect new requirements. Table 4 describes five basic characteristics of IDS systems and the corresponding changes that would have to occur.

Table 4. Modifications to IDS ssytems

IDS Characteristics	Current Requirement	Augmented to Embed Detective
System philosophy	Alert decision makers to a potential intrusion	Identify intrusion and begin forensic data collection
Detection methodology *Anomalous behavior*	Alerts when anomalous behavior occurs	Will require additional data to determine if anomaly is an intrusion
Signature detection	Alerts when known misuse/intrusion signatures detected	Collects forensic data when malevolent signature identified
Data storage	Random archiving and retention periods	Uniform archiving and retention periods
Sensor location	Near valuable data assets and strategic network nodes	Near assets determined by risk analysis to warrant a 4R strategy approach

Additional considerations might include:

1) Degree of autonomy in response—this will affect forensics in many ways, in that (a) the response itself may render forensic data inadmissible, (b) the response may require integration with a human to make decisions even in simple matters like handling the forensic data—not everyone may be legally authorized to see/handle all data, and (c) the response will more than likely cross domains, adding complexity to the task of the integrated detective.
2) Source of authority for data collection—the way data is gathered, who can see it, what data can be combined, etc, depends heavily on the source of authority for gathering that data as well as "who" gathered it. Does the detective make inferences based on all data? Does the detective decide not to pick up some data, or have an ability to request additional authority?

From our preliminary analysis, as users begin to automate more and more IDS/forensics systems, we have identified the issue of how IDS systems handle the legal and technological issues arising from cross/overlapping domains as an important research challenge to pursue.

4 Conclusions and Future Work

As courtroom admissibility requirements become important considerations for networked systems, 'embedding a detective in the network' is a useful metaphor for the changes that will be required. For systems to become forensically ready, substituting the 'embedded detective' for costly and non-scalable *ad hoc* investigations will necessitate a change in network protection strategies to include discovering the culprit, as opposed to simply restoring network function as quickly as possible when an intrusion occurs. The new strategy implies modification of existing security policies, tools, technologies and procedures to accommodate these additional requirements. A good example is IDS technology, which today provides some augmented cognition capabilities to network administrators, but will necessitate enhancement if the role of the detective is included.

We anticipate that organizations will find that selective implementation of forensic readiness is good security policy. Possible benefiting scenarios include pursuit of an insider/intruder for the purpose of legal action and documentation of due care in the event of civil litigation claiming networked systems are not adequately secured and defended.

Future work will involve:

1) Continued development of all phases of the NFDLC methodology.
2) Conceptualization and design of a forensically ready IDS system that embeds the skills of a detective.
3) Implementation of the NFDLC in a newly designed client network to assess the feasibility of limited forensic readiness.

References

1. Endicott-Popovsky, B.E., Ryan, D., Frincke, D.: The New Zealand Hacker Case: A Post Mortem. In: Proceedings Safety and Security in a Networked World: Balancing Cyber-Rights & Responsibilities, Oxford Internet Institute, Oxford, England (September 2005), Retrieved from the World Wide Web: http://www.oii.ox.ac.uk/research/cybersafety/?view=papers
2. Tan, J.: Forensic Readiness, @Stake, Cambridge, MA (2001)
3. Dittrich, D., Endicott-Popovsky, B.E.: INFO498 Introduction to Computer Security Incident Response, University of Washington, Seattle, WA (Fall, 2003)
4. Rowlinson, R.: Ten Steps to Forensic Readiness. International Journal of Digital Evidence 23(3) (Winter 2004)
5. Endicott-Popovsky, B.E., Chee, B., Frincke, D.: Role of Calibration as Part of Establishing Foundation for Expert Testimony. In: Proceedings 3rd Annual IFIP WG 11. Orlando, FL (January 2007)
6. Lawson, M, Lawson R.: Expert Witness Testimony. Global CompuSearch, LLC, Spokane, WA (2000-2003)
7. CSI/FBI: CSI/FBI Computer Crime and Security Survey, Computer Security Institute, San Francisco, CA (2005)

8. Bailey, K.: Trouble in Cyberspace: Why this Conference is Important, NWSec, Seattle, WA (February 2007), Retrieved from the World Wide Web http://students.washington.edu/greyhat/mainsec.html
9. Gates, P.: Seminar in Data Security, Seattle, WA (March 2005)
10. NIST: Computer Forensics Tool Testing (CFTT) Project, Retrieved from the World Wide Web: http://www.cftt.nist.gov/
11. Endicott-Popovsky, B.E., Frincke, D.: Adding the Fourth 'R': A Systems Approach to Solving the Hacker's Arms Race. In: Hawaii International Conference on System Sciences (HICSS) 39 Symposium: Skilled Human-intelligent Agent Performance: Measurement, Application and Symbiosis, Kauai, HI, (January 2006). Retrieved from the World Wide Web: http://www.itl.nist.gov/iaui/vvrg/hicss39/4_r_s_rev_3_HICSS_2006.doc
12. Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T.A., Mead, N.R.: Survivable Network Systems: An Emerging Discipline. CMU/SEI 97-TR-013, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA (May 1999)
13. Mocas, S.: Building Theoretical Underpinnings for Digital Forensics Research. Compsec Online: Digital Investigations 1(1) (2003)
14. Endicott-Popovsky, B., Frincke, D.: Embedding Forensic Capabilities into Networks: Addressing Inefficiencies in Digital Forensics Investigations. In: Proceedings Seventh IEEE Systems, Man and Cybernetics Information Assurance Workshop, pp.133–139. United States Military Academy, West Point, NY (June 2006)
15. Grance, T., Hash, J., Stevens, M.: Security Considerations in the Information System Development Life Cycle. U.S. Department of Commerce, NIST Special Publication, pp. 800–864 (2004)
16. Bailey, K., Winn, J.: Personal Interviews (March 2006)
17. Yasinsac, A., Manzano, Y.: Policies to Enhance Computer and Network Forensics. In: Proceedings 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY (June 2001)
18. Wolfe-Wilson, J., Wolfe, H.B.: Management Strategies for Implementing Forensic Security Measures (electronic version). Information Security Technical Report 8(2), 55–64 (2003)
19. Carrier, B., Spafford, E.: Getting Physical with the Digital Investigation Process [electronic version], International Journal of Digital Evidence, vol. 2(2) (Fall 2003)
20. Endicott-Popovsky, B.E., Fluckiger, J.D., Frincke, D.A.: Establishing Tap Reliability in Expert Witness Testimony: Using Scenarios to Identify Calibration Need. In: Proceedings 2nd International Workshop on Systematic Approaches to Digital Forensic Engineering, Seattle, WA, (April 2007)