A Theoretical Framework for Organizational Network Forensic Readiness

Barbara Endicott-Popovsky
University School, Seattle, USA
Email: endicott@u.washington.edu

Deborah A. Frincke
Pacific Northwest National Laboratory, Richland, USA
Email: deborah.frincke@pnl.gov

Carol A. Taylor
University of Idaho
Email: ctaylor@cs.uidaho.edu

***Abstract*—This paper discusses breaking the escalation cycle that locks cyber intruders and their targets in a state where targets are perennially resigned to attacks and intruders are at liberty to exploit and disrupt networks without much risk of suffering consequences. Using systems and case analyses, several research questions are explored, resulting in the identification of conditions that must change in order to interrupt this unproductive relationship between attackers and targets. As an outcome, network forensic readiness (NFR) is proposed as a solution to digital forensic investigations that have become too resource intensive to encourage broad application to the growing numbers of computer crimes. While NFR has been implemented to some degree through tools, procedures and checklists, no comprehensive organizational implementation approach has been identified. Thus, a theoretical framework is offered as a basis for "operationalizing" network forensic readiness. The framework includes several models for implementing NFR in the enterprise.**

Index Terms—**digital forensics, networks, network forensics**

I. Introduction

A typical incident response presents time-pressured technicians with networks that provide little support for forensic data collection [1, 2]. They often must choose between seeking to gather network data in such a way that it *may* be "forensically sound," or restoring the network as quickly as possible [3]. When "forensic soundness" includes the ability to stand up to legal scrutiny in a court of law, the effort involved can be extremely expensive in labor and time, and even at that, the effort may not be successful, or utilized. The requirement to restore productivity often drives technicians to network restoration, even when the result is alteration of key files, limiting their forensic value, including value as courtroom evidence.

When there continues to be relatively limited interest in pursuing legal action [4,5], the rational choice for those administering networks often is the expedient one—restore productivity by restoring network function as rapidly as possible, and applying minimal effort to collecting and preserving forensically sound information for later courtroom use.

The concept of network forensic readiness (NFR), defined as "maximizing the ability of an environment to collect credible digital evidence while minimizing the cost of an incident response," arose in this context as a recommendation for improving the efficiency of investigations [1]; however, to date, there has been little discussion of how to fully integrate NFR into networked systems, aside from recommending the use of specific tools, checklists, etc. This paper offers a comprehensive methodology for embedding forensic capabilities into networks, thus 'operationalizing' NFR. It begins by exploring the context for network investigations, including an analysis of two well-documented cases of malicious intrusion, and then develops a theoretical basis for including NFR among operational security strategies. We conclude with a discussion of the NFDLC methodology, focusing on the direction the work is taking.

This research direction began by asking: '*What maintains the status quo between attackers and targets*?'

II. Research Question 1:

What Maintains the *Status Quo*?

The expedient approach to incident response—restore system function quickly, ignoring procedures for collecting forensically sound data—exists in a context of what has been described as an "arms race" with network intruders [6]:

Based on ""Embedding Forensic Capabilities into Networks: Addressing Inefficiencies in Digital Forensics Investigations" by B.E. Endicott-Popovsky and Deborah Frincke, which appeared in the Proceedings of the 7th IEEE Workshop on Information Assurance 2006, U.S. Military Academy, West Point, USA, June 2006. © 2006 IEEE.

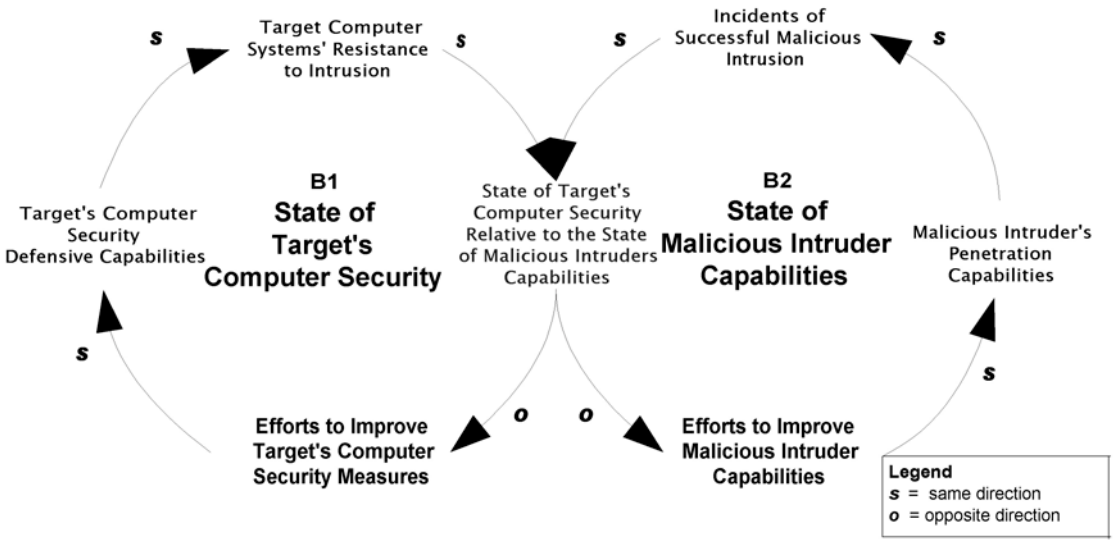

Figure 1. "Arms race" escalation cycle [adapted from 8,9,10]

Reading Figure 1, as information system defenses improve, malicious intruders' skills must also improve in order to continue to wage successful attacks. As attacker skills improve, targets improve system security to repulse attacks in a continuous pattern of escalation [6]. What continues to fuel this cycle is mutually perceived gaps between the state of a target system's security and intruders' abilities.

Several trends add fuel to this system:

- The volume of cyber attacks continues to increase, and it takes less technical knowledge to launch increasingly sophisticated attacks, using increasingly sophisticated hacker tools [7].
- The threat spectrum is growing; recreational hackers are being displaced by organized crime and nation states [8].
- Organizations are becoming increasingly reliant on public networks, often without tempering enthusiasm with a concern for security [11].
- Surveys continue to report increased organizational investments in tools and techniques that protect information systems and prevent intrusions in response, yet criminal intrusions are escalating in numbers and severity [12].

In spite of the growth trends, deterring crime by inviting law enforcement to participate in intrusion investigations is not a strategy pursued by many organizations. As a result, few incident response investigations are undertaken with the objective of holding intruders liable, and fewer of those that have that objective result in successful prosecution [13].

The initial research question prompting this study was *'what maintains the status quo?'* The conditions described above should be untenable, causing organizations to adopt a strategy of pursuing legal deterrence.

Reasons for an aversion by organizations to pursue legal options [14,15] include:

- Concern for the organization's reputation if incidents become public knowledge
- Concern for balance sheet and share price impacts from contingent liabilities related to public awareness of network intrusions
- Concern for loss of revenue if consumer confidence in the security and privacy of their data residing in the organization's systems erodes.
- Fear that law enforcement will seize computing equipment and consume resources once an investigation begins.

To gain further insight, two well-documented cases of criminal intrusion were examined and analyzed.

A. Case Analyses

The New Zealand and Russian Hacker Cases were selected for comparative analysis because extensive data was available for each, and each involved a law enforcement investigation as part of incident response. Facts about each case and the corresponding network forensic investigation were compared in [16]. Results are summarized in Table I.

TABLE I: COMPARING THE NEW ZEALAND AND RUSSIAN HACKER CASES

	Characteristics	New Zealand Hacker Case	Russian Hacker Case
Facts related to case	**Type of attack**	Typical intrusion scenario (Figure 2)	Automated online auctions using stolen credit card #'s (Figure 3)
	Intruders	Recreational hackers	Criminal hackers
	Damages	$400,000	$25 million
Facts related to network forensic investigation	**Motivation to involve law enforcement**	Number of machines and organizations impacted	Extent of threats and impacts to one victim organization
	Investigator time	417 hours	9 months
	Investigation costs	$27,800 (*1 victim only*)	$100,000 (*partial estimate*)
	Consequences	No prosecution	3 & 4 years in Federal prison less time served
	Investigator	Sys admin learning forensics	Expert recruited to work full time for the FBI
	Network Forensic readiness	Reactive *Ad hoc*	Reactive *Ad hoc*

B. New Zealand Hacker Case Summary

The New Zealand Hacker Case has been described as the "largest security incident in New Zealand history" [17] with damages estimated at $400,000 [18]. Evidence indicated that several intruders were involved, physically located in several countries including New Zealand and the United States [2]. The attackers executed a typical intrusion scenario (Figure 2) [19], exploiting a buffer overflow to gain root access and install root kits and back doors for unfettered future access [20,21].

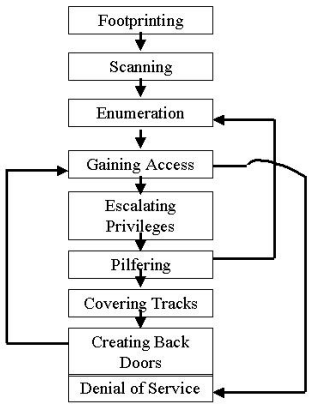

Figure 2. Typical intrusion scenario [19]

Once within the network perimeter, they set up new accounts and installed network sniffers to capture logins and passwords [2]. Then compromised machines were used as stepping-stones for attacks on other machines, often employing a several-hop pattern to disguise the actual origin of their attacks before getting to the desired target [2].

Over 4,000 user websites were disabled or defaced, along with over 500 commercial sites [17]. One victim documented investigation costs of $27,800 ± $4200, including 417 hours of investigator time—one quarter of a man-year[1]. [22] The investigator (a systems administrator learning forensics during the investigation) worked closely with law enforcement. Ultimately, there was no prosecution since, at the time, there were no New Zealand laws making this a crime. [2]

C. Russian Hacker Case Summary

The Russian Hacker Case is considered "one of the largest and most complex cases of criminal intrusion using public networks to have gone from forensic investigation through a successful verdict" [15]. The Russian criminals in this case conducted a variety of online illegal projects. The one prosecuted was a virtual business that automated both sides of fabricated e-Bay auctions using Perl scripts that triggered payments to PayPal and a stolen database of credit card numbers (Figure 3) [23,24].

Working with an ISP victim, the FBI created a fictitious "startup company" that invited the intruders to Seattle to 'interview for security jobs' and demonstrate their hacking prowess—providing the FBI with incriminating evidence [24]. They were arrested and later tried and convicted, respectively, in two different jurisdictions in a joint prosecution involving U.S. Attorneys Offices in several states [23,24,25]. V. Gorshkov was sentenced in Seattle on October 4, 2002 to three years in Federal prison; A. Ivanov, on July 24, 2003, to four years in Federal prison in Hartford, Connecticut [26,27]. They were credited for time served, reducing their sentences by two years.

[1] Costs incurred by one victim's investigator, exclusive of those incurred by law enforcement.

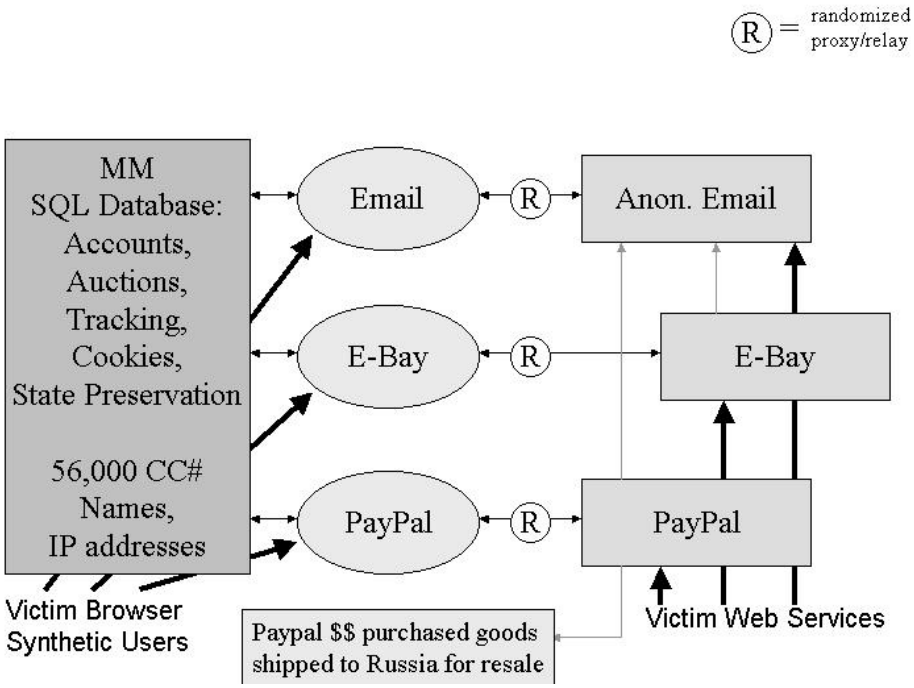

Figure 3. Virtual criminal enterprise [23, 24]

Victim losses in the automated auction scam were estimated at $25 million [23,24,25]. The primary digital forensic investigator was recruited from industry and worked full time for approximately nine months developing the case [15]. Fully burdened, his time is estimated at $100,000. Total costs were significantly greater; however, those of law enforcement have not been made available [24].

Investigations in both cases were conducted in an *ad hoc*, reactive mode. They tied up valuable resources better employed elsewhere, particularly given the legal outcomes; and neither the investigators, nor networks, were adequately prepared to support such investigations, efficiently [13,16]. Given the level of effort required, it was concluded in [16] that such approaches are not sufficiently scalable to address a significant number of intrusion cases.

The authors contend that changing the state of the practice of digital forensics from reactive to proactive necessitates the inclusion of a willingness to prevail in the courtroom among an organization's computer security management policies—which will lead to investment in changes to the way networks are managed [28]. While some practitioners report relatively little demand for such improvements [11,13,22], the combination of new legislation[2] and the increase in cyber crime is causing legal counsel to urge clients to devote new resources to fund procedures and technology that will allow collection of forensically sound data, defensible in a court of law [29].

Thus, answering Research Question #1, a major reason legal remedies are not pursued in cyber intrusion cases, is the cost and level of effort required for reactive investigations. Expecting increased motivation to pursue legal action, the question then becomes: *'How can these inefficiencies be reduced?'*

III. Research Question 2: How Can Network Forensic Investigation Inefficiencies Be Reduced?

The discipline of network forensic readiness (NFR) has emerged in this context of high costs for investigating malicious online intruders [1]. As Tan suggests, if part of the investigatory process becomes embedded—substituting for time spent developing evidence by highly skilled, specifically trained individuals—then it seems logical that greater efficiencies will result [1].

To date, realization of network forensic readiness in organizations has been fragmented [3]. While tools and techniques have been developed, there has as yet been no comprehensive, enterprise-wide framework for implementation:

[2] e.g., Sarbanes-Oxley, the Health Information Portability and Privacy Act (HIPPA)

1) Researchers who have developed tools that implement some aspects of NFR include:

- Yasinsac and Manzano, who proposed six categories of policies to enhance network forensics in enterprises [30],
- Wolfe-Wilson and Wolfe, who recommend planned procedures for incorporation into existing incident response plans [31],
- Carrier and Spafford, who describe a readiness phase that ensures support for forensically sound investigations [32],
- Rowlinson, who goes further, proposing a 10-step process for instantiating NFR [33],
- Tang and Daniels, who proposed a simple technical framework for a forensic-ready network [34].

2) In addition, organizations have developed incident response procedures, enabling legal pursuit for [35]:

- Collecting evidence in a manner that supports courtroom admissibility,
- Following chain of custody procedures for storing evidence,
- Establishing escalation procedures that identify when to invite law enforcement, etc.

While certain elements of network forensic readiness have been defined, a comprehensive approach remains lacking [36,37,38].

As validation, Table II summarizes the distribution of research topics presented at the Digital Forensics Research Workshops (DFRWS) from 2002 to 2006, demonstrating the emphasis on tools, techniques and methods, as opposed to an integrated, comprehensive solution [5, 36]. As one of the premiere venues for digital forensics research, the DFRWS typifies the scientific research focus in the field to date

TABLE II. DISTRIBUTION OF PRESENTATIONS DFRWS 2002-2006

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

One of the challenges to developing an enterprise solution is that digital forensics has been perceived as belonging to the realm of law enforcement, not necessarily to systems or network administration [36]. When an incident occurs, the FBI is brought in to do an investigation when there is a desire to pursue the criminal/s responsible [2,5].

Implementing NFR in an organization will require accepting an expanded role for systems and network administrators, as well as an understanding of how legal requirements for admissible evidence can be translated into information system requirements—i.e., what network data to collect and where; what tools and procedures to use and how; who should be trained and in what topics; etc. Adopting a tool or technique, alone, will not be sufficient.

After identifying network forensic readiness as a solution to the inefficiencies of today's digital forensic investigations and recognizing the lack of a comprehensive approach, the next research question emerges: *'How can NFR be implemented in the enterprise?'*

IV. RESEARCH QUESTION 3: How Can Network Forensic Readiness be Implemented in the Enterprise?

To answer this question and fill the research gap, the authors propose a theoretical framework for digital forensics that includes enterprise implementation models [3,4,6].

A. Theoretical Base for Digital Forensics

In [6] it was suggested that digital forensics should be integrated into the discipline of information assurance as one of its methods. As defined by McCumber, creator of a widely accepted definitional model of Information Assurance, security countermeasures are the technologies, policies/practices and human factors (training, vetting employees, etc.) that implement information assurance [39,40]. These countermeasures are deployed through the three basic information states—transmission, storage and processing; providing three services to systems—confidentiality, integrity and availability The authors propose that digital forensics has a function within each cell of the cube (Figure 4), giving it a role in enterprise information systems operations [28].

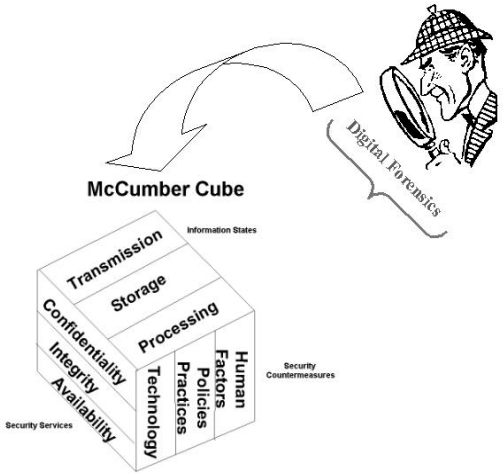

Figure 4. Integrating digital forensics in information assurance [39, 40]

Thus defining what it means for a specific network to be "forensically ready" incorporates the full spectrum of information assurance (IA) elements—security policies,

procedures, practices, mechanisms, and security awareness training programs.

Figure 5 presents a conceptual framework for embedding digital forensics in the enterprise, where policies, procedures, practices, mechanisms, and awareness training are driven by a system goal expressed as 'preserving the ability to prosecute malicious cyber intrusion successfully, while reducing current effort expended on digital forensic investigations.'

Applying this model, the goal leads to development of appropriate management policies with respect to all aspects of forensics, such as support for evidence gathering. These policies then are implemented through corresponding procedures/practices and/or mechanisms, which in turn provide the basis for security awareness training throughout the enterprise to disseminate security policies and instruction about their implementation. The result is a forensically ready network. As a feedback mechanism, IA audit communicates the effectiveness of the various elements to decision makers who make appropriate adjustments, as needed.

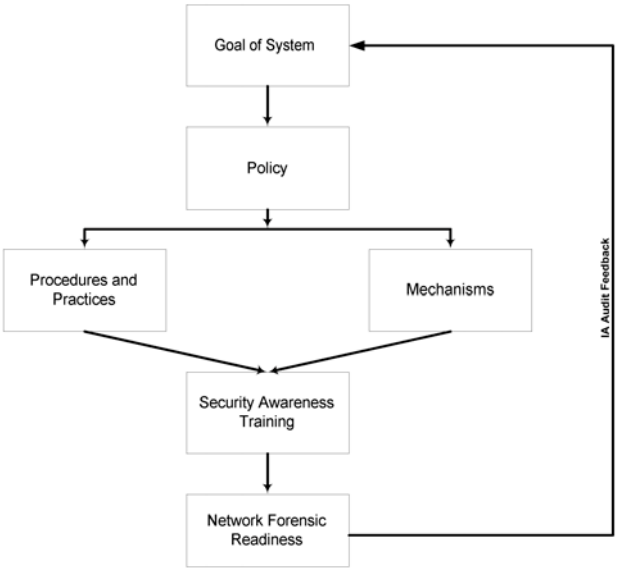

Figure 5. Conceptual framework for embedding digital forensics in the enterprise,

Application of this model assumes a management policy of holding intruders accountable, which, as stated earlier, is not usually the case [6]. Therefore the authors offer the conceptual 4R model for Accountable Systems to guide development of the strategies necessary for implementing forensically ready networks.

B. Strategy Model to Aid Policy Development

If increased prosecution of cyber crimes is to occur, organizations must be willing to adopt a policy of holding intruders accountable. Reluctance to do so to date is reflected in the 3R model (Table III) for Security Strategies of Survivable Systems (from the survivability discipline [41]).

TABLE III STRATEGIES OF SURVIVABLE SYSTEMS

Survivability 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 or 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 • Replication • Backup systems • Fault tolerant designs

The traditional approach to managing networks is embodied in this model and can be characterized as systems administrators resigned to attacks and forensic investigations focused on discovering what happened (as opposed to who did it) so systems can be patched and restored quickly. The three strategies—**R**esistance, **R**ecognition and **R**ecovery—and their corresponding tools, summarize the techniques used to secure networks today. All are defensive in nature, assuming the inevitability of attack.

To offer a strategic approach that would include holding perpetrators responsible, the 4R Model for Strategies for Accountable Systems was developed as an adaptation (Table IV) [6].

TABLE IV 4R STRATEGIES OF ACCOUNTABLE SYSTEMS

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 in a court of law. 2) Ability to retaliate	• Forensics - *the who* • Legal remedies • Active defense

The first three strategies—**R**esistance, **R**ecognition and **R**ecovery—remain. The additional 4th R—**Redress**—defined as the ability to hold intruders accountable, provides additional tools including digital forensics, legal remedies and active defense.

While forensics (small "f"), is part of **R**ecovery in the 3R model [6], it is not rigorous enough for capturing evidence admissible in a courtroom, with its focus is on discovering *what* happened in order to restore network function quickly [4]. **Redress** requires computer Forensics (capital "F"), which focuses on establishing

who is responsible in order to develop suitable evidence to hold them accountable in a court of law.[3]

Adopting the 4R strategy model provides a conceptual basis for developing information assurance policies that include digital forensics. By implication, it expands the duties of those securing networks to include identifying digital forensic requirements when developing information system procedures, practices and mechanisms [43]. To accomplish this, the authors offer a life cycle methodology for embedding forensics in networked systems.

C. Life Cycle Model

A 4R strategic approach requires re-examination of current security procedures, practices and mechanisms for compliance with more rigorous evidence collection, storage, and admissibility standards [4,6]. In [3], we introduced a methodology for embedding forensic readiness in information systems, based on the NIST Information Systems Development Life Cycle (ISDLC), which was devised to incorporate security across the life cycle of systems development [44].

If information assurance is redefined to include digital forensics, then a methodology that develops secure systems should also be a vehicle for delivering forensic capability, as depicted in Figure 6 where the 4R approach informs each phase of the ISDLC. Design of such a system should take into consideration the necessary legal requirements for compliance with evidence collection and storage standards for courtroom admissibility and affect each phase of the life cycle.

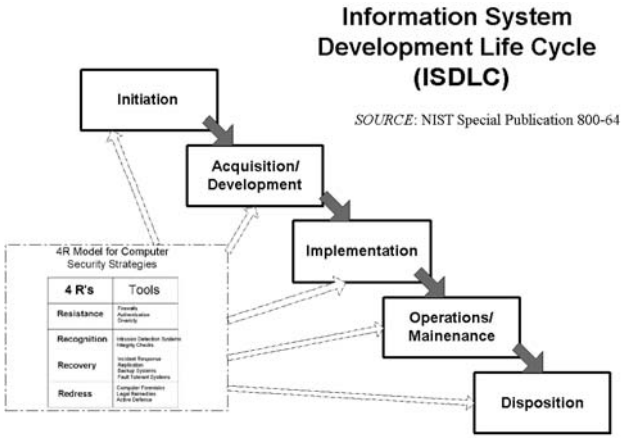

Figure 6 The ISDLC as a vehicle for delivering digital forensic functionality

During a study of the ISDLC methodology, each phase was analyzed and modified to include additional steps that ensure embedding of digital forensic functionality. The content modifications required in each phase produced the Network Forensics Development Life Cycle (NFDLC) in Figure 7.

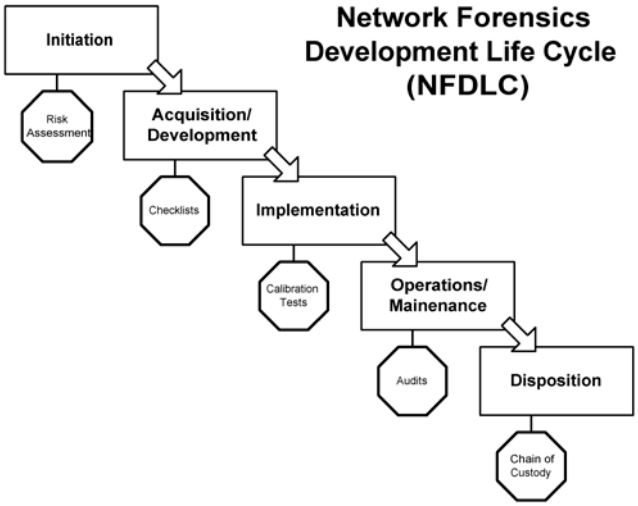

Figure 7 NFDLC Methodology

The specific ISDLC modifications that produce the NFDLC are summarized in Table V and subsequently described:

TABLE V NFDLC PROCEDURAL CHANGES TO ISDLC PHASES

ISDLC (Life Cycle) Phases	NFDLC Additional Procedures
Initiation Phase: preliminary risk assessment	Determine what aspects of a network would warrant digital forensic protection
Acquisition/Development Phase	Adhere to Rules of Evidence in system requirements Apply published forensic checklists [i.e.31, 32, 33]
Implementation Phase	Perform baseline testing Perform network/mechanism verification/calibration tests
Operation/Maintenance Phase	Conduct verification/calibration audits
Disposition Phase	Incorporate chain of custody/evidence preservation procedures

1) Initiation Phase: Additional steps to the preliminary risk assessment would include determination of what assets on the network would warrant digital forensic protection. In other words, what assets of the organization justify pursuit of legal redress if deliberately compromised? In preliminary conversations with practitioners, such a selective approach would limit the initial cost and administrative burden associated with forensic readiness [45,46].

2) Acquisition/Development Phase: System requirements would be generated that would include assurance that any device or procedure collecting forensic data on the system will do so in a manner compliant with courtroom standards [4]. Analysts in this phase might

[3] In [42], Sommers makes the distinction between small "f" *computer forensics*, an investigatory activity to discover *what* happened prior to restoring computer systems that have been attacked, and *computer Forensics* with a capital "F," which additionally seeks to validate the identification of *who* was involved, by using techniques for gathering and preserving evidence that will be upheld in a court of law.

find previously published checklists [i.e., 32,33,34] useful to determine what existing forensic procedures/tools/technologies could be embedded, building on prior research.

3) Implementation Phase: Calibration tests are recommended to verify the performance of devices used to collect evidence and to document the performance of the network itself. This would be accomplished by first baselining the network, or network segment, being made forensically ready. Network baselining" is "the systematic analysis of a network, point to point, for dataflow, communication sequencing, performance statistics, etc." [47]. This would be followed by calibration/verification of the performance of network devices involved in collecting evidence in order to understand how they behave across a range of characteristics [4] Calibration is the "determination of the accuracy of an instrument, usually by measurement of its variation from a standard" and is useful in establishing foundation evidence that tools used for forensic evidence gathering function as intended [4,48].

4) Operation/Maintenance Phase: Audits would be performed at regular intervals, and as the network grows and changes, to confirm results of previous baseline and verification/calibration tests. Documentation would be generated and maintained as evidence that the network and forensic devices continue to function properly, recording any adjustments that were necessary.

5) Disposition Phase: Chain of custody procedures would be incorporated into this phase to ensure preservation of the value of potential evidence residing in a retired system.

D. External Validation

Informal interviews were conducted with practitioners to gauge their perception of the theoretical and implementation models presented here, as well as to determine their interest in participating in a proof of concept [45,46]. The following feedback provided assurance of the value of this approach:

1) To the extent that forensic capabilities are embedded in networks, it was agreed that forensic investigations most likely will require less investigator time and effort.
2) However, this may be balanced by the fact that the more forensic data is collected from networks in the course of business, the more legal discovery requests may arise, inflicting additional time and resource penalties.
3) Nevertheless, key data assets on the network warrant the protection that embedded forensic capabilities can provide.

Summarizing the interviews, it appears that two scenarios might benefit from an embedded forensic capability: 1) the pursuit of a malicious intruder, or internal misuser, for the purpose of criminal prosecution or administrative action and 2) documentation of due care in the event of civil litigation claiming that networks are not adequately defended.

The former would require broader dispersal of embedded forensic capability throughout the network, since the path of an intruder or misuser through a network is unpredictable. The latter would limit the investment in embedded forensic capability to those parts of the network in proximity to critical data assets that have network access and where the enterprise has a duty of care.

V. CONCLUSIONS

This paper has shown that current approaches to digital forensics are not scalable to handle the growing numbers of cyber crime cases—therefore greater efficiency is needed. The implication is that the current practice of collecting digital forensic evidence is more of an art than a science through the use of unrepeatable, often *ad-hoc* procedures, the results of which could lead to evidence of questionable quality that can be challenged in the courtroom.

One suggested solution is Network Forensic Readiness (NFR), essentially embedding forensic capabilities in networks, minimizing the reliance on highly skilled and trained individuals while maximizing the ability to collect forensically sound information. Forensic readiness proposes that systems be designed or enabled to capture forensic evidence beyond their current capabilities. The idea has been endorsed within the forensics research community, but its implementation has yet to be realized beyond individual tools, techniques and methods [3,4,6]. The need was identified for a comprehensive, systemic approach to implementation in the enterprise.

The theoretical framework presented will provide the basis for developing a forensically ready organizational network. The framework includes the Conceptual Framework for Embedding Digital Forensics in the Enterprise, the 4R Strategies of Accountable Systems and the Network Forensics Development Life Cycle (NFDLC), a model that extends NIST's ISDLC by embedding digital forensic functionality at each stage. Together they provide a toolset for implementing forensic readiness enterprise-wide.

VI. FUTURE WORK

Future work involves further definition of the NFDLC methodology beginning with continued development of calibration standards and techniques, followed by the creation of formalisms that define forensic readiness system policies. Once fully developed, the methodology, along with the approaches and models just discussed, will be applied to a network design problem in order to determine whether it resolves Research Question #3 by successfully implementing network forensic readiness in an enterprise.

Calibration testing from the Implementation Phase of the NFDLC was identified for initial attention because existing network devices, such as switches and taps with span port capability, are already employed to collect network traffic data for courtroom presentation. Without validation of their performance through calibration, any forensic evidence these devices collect can be challenged by opposing counsel, devaluing its reliability to a jury or even leading to inadmissibility [4].

A generalized model for designing calibration tests for low layer network devices and an exemplar test case of an aggregator tap are described in [4]. Additional work is needed to extend this model to more complex network devices and to assist in the development of a standard calibration protocol.

Concurrent with this avenue of exploration, the authors are developing a system forensics policy as part of the NFDLC Initiation Phase where requirements are delineated. Having a clearly stated forensics policy for a system has many potential benefits including clearly defined policy enforcement mechanisms, well-defined risks, and consequences should the forensics policy be violated. Another benefit of having a forensics policy is that the policy can be stated formally, in mathematical notation, which allows for formal proof that a system is capable of satisfying its forensics policy.

The approach taken to forensics policy modeling is based on the large body of security policy research over the past thirty years. The security research community has shown that formal, as opposed to natural language, models allow unambiguous representation of a policy and greater preciseness in both model definition and meaning. Consequently, while the first introduction of the concept of a forensics policy is in a natural language form, the work will progress to a formal representation of the policy. Proof techniques will also be demonstrated in verifying the correctness of a system that would uphold the formal forensics policy.

A candidate case for applying the approaches outlined in this paper has already been selected. The organization involved develops networks for clients who have a need for forensic readiness. It is expected that implementation using the approaches previously discussed will provide useful feedback for further refining the models and methodology.

ACKNOWLEDGMENT

The authors wish to thank John Dickinson, formerly of the University of Idaho, for the inspiration and support he provided during his lifetime.

REFERENCES

[1] Tan, J. (2001). "Forensic Readiness," Cambridge, MA: @Stake.

[2] D. Dittrich and Endicott-Popovsky, B.E. (Fall, 2003). "INFO498 Introduction to computer security incident response," University of Washington, Seattle, WA.

[3] Endicott-Popovsky, B and Frincke, D., "Embedding forensic capabilities into networks: addressing inefficiencies in digital forensics investigations" in *Proceedings from the Seventh IEEE Systems, Man and Cybernetics Information Assurance Workshop,* 21-23 June 2006, United States Military Academy, West Point, NY, pp.133-139.

[4] Endicott-Popovsky, B.E., Chee, B. and Frincke, D. "Role of calibration as part of establishing foundation for expert testimony," in *Proceedings 3rd Annual IFIP WG 11.9 Conference,* January 29-31, Orlando, FL.

[5] Orton, I. "Coordinating with law enforcement on security issues," presented at *Computer Security and Cybercrime II: Legal Risks and Responsibilities in a Dangerous World Workshop*, King County Bar Association, October 24, 2002, Seattle, WA

[6] Endicott-Popovsky, B.E., Frincke, D. "Adding the Fourth 'R': A systems approach to solving the hacker's arms race." *Hawaii International Conference on System Sciences (HICSS) 39 Symposium: Skilled Human-intelligent Agent Performance: Measurement, Application and Symbiosis*, 4 January 2006, Kauai, HI, Retrieved Feb. 17, 2007 from the World Wide Web: http://www.itl.nist.gov/iaui/vvrg/hicss39/4_r_s_rev_3_HICSS_2006.doc.

[7] Carnegie-Mellon Software Engineering Institute CERT Coordination Center. (2007). "CERT/CC Statistics 1988-2006." Retrieved Feb. 17, 2007 from the World Wide Web: http://www.cert.org/stats/cert_stats.html.

[8] Senge, P. M. (1990). *The Fifth Discipline.* New York: Doubleday Currency.

[9] Senge, P., Roberts, C., Ross, R.B., Smith, B.J.,& Kleiner, A. (1994). *The Fifth Discipline Fieldbook: Strategies and Tools for Building a Learning Organization.* New York: Doubleday-Currency.

[10] Kim, D. H. (1992). *Systems Archetypes I: Diagnosing Systemic Issues and Designing High Leverage Interventions.* Waltham, MA: Pegasus Communications, Inc.

[11] Kirk Bailey, "Trouble in cyberspace: Why this conference is important," presented at *NWSec,* February 15, 2007, Seattle, WA, Retrieved Feb. 17, 2007, from the World Wide Web: http://students.washington.edu/greyhat/mainsec.html

[12] CSI/FBI: CSI/FBI. (2005)."Computer crime and security survey," Computer Security Institute, San Francisco, CA.

[13] Ivan Orton, King County Deputy Prosecutor. *Personal interviews*. August 24, 2006 and September 29, 2006.

[14] Oman, P., Schweitzer, E. and D. Frincke, "Concerns about intrusions into remotely accessible substation controllers and SCADA systems," presented at the *27th Annual Western Protective Relay Conference, 23-26 Oct.ober, 2000*, Spokane, WA.

[15] Schroeder, S., Federal prosecutor (Retired) (Spring, 2004). *CSSE592 Computer forensics: Legal overview*, Seattle University, Seattle, Washington.

[16] Endicott-Popovsky, B.E., Ryan, D., Frincke, D. (2005). T*he New Zealand hacker case*: "A post mortem," in *Proceedings of the Safety and Security in a Networked World: Balancing Cyber-Rights & Responsibilities Conference at the Oxford Internet Institute*, 8-10 September, 2005, The University of Oxford, Oxford, England. Retrieved Feb 17, 2007 from the World Wide Web: http://www.oii.ox.ac.uk/microsites/cybersafety/?view=papers

[17] Barton, C. "Hacker destroys 4500 web sites," *New Zealand Herald*, November 19, 1998, Retrieved August 13, 2005 from the World Wide Web: http://www.landfield.com/isn/mail-archive/1998/Nov/0098.html

[18] Wall, T. "Associates denounce website hacker," *New Zealand Herald*, November 23, 1998, Retrieved August 13, 2005 from the World Wide Web: http://www.landfield.com/isn/mail-archive/1998/Nov/0098.html

[19] McClure, S., Scambray, J. and G. Kurtz. (2003). *Hacking Exposed: Network Security, Secrets & Solutions*. (4th ed.) New York: McGraw-Hill.
[20] CERT® "Incident Note IN-98.04: Advanced scanning." Retrieved August 02, 2005 from the World Wide Web: http://www.cert.org/incident_notes/IN-98.04.html
[21] Honeynet Project. (2000). "Know your enemy III: They gain root." Retrieved August 04, 2005, from the World Wide Web: http://project.honeynet.org/papers/enemy3/index.html
[22] Dittrich, D. "Developing an effective incident cost analysis mechanism," *Security Focus*, June 12, 2002. Retrieved August 14, 2005 from the World Wide Web: http://online.securityfocus.com/infocus/1592
[23] Attfield, P., "Real-world access control systematic failures: Reality or virtual reality," in *Journal Article Workshop*, June '05, Ukraine.
[24] Schuler, M and P. Attfield. (April 18, 2002). "Seattle FBI briefing: Operation Flyhook," *Boeing Security Forum*, Seattle, WA.
[25] Koerner, B. "From Russia with Lopht." *Legal Affairs*, May 1, 2002. Retrieved August 7, 2005 from the World Wide Web: http://www.newamerica.net/index.cfm?pg=article&DocID=792
[26] United States. Department of Justice. "Court proceedings and public-record trial exhibits," United States v. Vasily Gorshkov. Seattle, WA, September 2001.
[27] United States. Department of Justice. "Press release: Russian hacker sentenced." Newark, NJ, July 25, 2003. Retrieved August 7, 2005 from the World Wide Web: http://www.usdoj.gov/criminal/cybercrime/ivanovSent_NJ.htm
[28] Endicott-Popovsky, B.E., Frincke, D. *Redefining Computer Security to Include Forensics*, Poster session, 8th Annual Recent Advances in Intrusion Detection (RAID) Conference 7-9 September 2005, Seattle, WA.
[29] Simon, M. *Seminar in Data Security*. Preston Gates: Seattle, WA, March 2, 2005.
[30] Yasinsac, A. and Manzano, Y. (2001) "Policies to enhance computer and network forensics." *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*. June 2001, United States Military Academy, West Point, NY.
[31] Wolfe-Wilson, J. and Wolfe, H.B. (2003) "Management strategies for implementing forensic security measures "[electronic version]. *Information Security Technical Report* Volume 8, Issue 2, June 2003, pp.55-64.
[32] Carrier, B. and Spafford, E. "Getting physical with the digital investigation process," *International Journal of Digital Evidence*, vol. 2, 2 [Electronic version] Fall 2003.
[33] Rowlinson, R. "Ten steps to forensic readiness," *International Journal of Digital Evidence*, Winter 2004, Volume 2, Issue 3.
[34] Tang, Y. and T. Daniels. "A simple framework for distributed forensics." *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops*, June 2005, Columbus, Ohio.
[35] Schultz, E.E. and Shumway, R. (2002). *Incident Response: A Strategic Guide to Handling Systems and Network Security Breaches*, Indianapolis, IN: Sams Publishing.
[36] Pollit, M. Unit Chief FBI CART (Retired), *Personal interview*, July 12, 2005, Syracuse, New York.
[37] Mocas, S., (2004). "Building theoretical underpinnings for digital forensics research," *Compsec Online*: *Digital Investigations*. Vol. 1, Issue 1.
[38] Rogers, M. and K. Siegfried. (2003). "The future of computer forensics: A needs survey," *CERIAS Tech Report 2003-30*, Purdue University, Layfayette, IN.
[39] Maconachy, V., Schou, C., Ragsdale, D. and D. Welch, "A model for information assurance: an integrated approach," in *Proceedings of the 2nd Annual IEEE Information Assurance Workshop*, June 2001, USMA, West Point.
[40] McCumber, J. (1991). "Information systems security: A comprehensive model," in *Proceedings of the 14th National Computer Security Conference*, Washington, D.C., October, 1991; reprinted in the *Proceedings of the 4th Annual Canadian Computer Security Conference*, Ottawa, Ontario, May, 1992; reprinted in *DataPro Reports on Information Security*, Delran, NJ: McGraw-Hill, 1992.
[41] Ellison, R.J., Fisher, D.A., Linger, R.C., Lipson, H.F., Longstaff, T.A. and. N.R. Mead. (May, 1999). "Survivable network systems: An emerging discipline. CMU/SEI 97-TR-013," Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, PA.
[42] Sommers, P. "Emerging problems on digital evidence." Presented at the *Computer Forensics Workshop*, September, 2002, University of Idaho, Moscow, ID.
[43] Ryan, D. "New directions in cyber law. Paper," Presented at the *CISSE 7th Colloquium*. June 2003, Washington, D.C.
[44] Grance, T., Hash, J. and Stevens M. (2004). "Security considerations in the information system development life cycle." U.S. Department of Commerce, NIST Special Publication 800-64. Retrieved from the World Wide Web Feb. 17 2007:
http://csrc.nist.gov/publications/nistpubs/index.html
[45] Bailey, K., Chief Information Security Officer University of Washington, and Winn, J., Director of the Shidler Center for Law Commerce and Technology, University of Washington, *Personal interviews*. Seattle, WA March 31, 2006.
[46] Simon, M. Chief Technology Officer, Conjungi Corporation, *Personal interviews*. Conjungi: Seattle, WA, Summer, 2005.
[47] Nassir, D. (2000). *Network Performance Baselining*. MTP: Indianapolis, IN, p.1.
[48] W. B. Saunders Harcourt Health Sciences. "Definition: calibration," Retrieved from the World Wide Web July 31, 2006.
http://www.mercksource.com/pp/us/cns/cns_hl_dorlands.jspzQzpgzEzzSzppdocszSzuszSzcommonzSzdorlandszSzdorlandzSzdmd_c_03zPzhtm

Barbara Endicott-Popovsky (Pittsburgh, Pennsylvania) She is a Ph.D. candidate in computer science at U. Idaho, Moscow, ID, USA, (Summer 2007); She has an MS in information systems engineering from Seattle Pacific University, Seattle, WA, USA (1987); and an MBA from the University of Washington, Seattle, WA, USA (1985), and a BA in Liberal Arts from the University of Pittsburgh, Pittsburgh, PA, USA (1967).

She is the Director of the Center for Information Assurance and Cybersecurity at the University of Washington, Seattle, WA, USA, with a joint faculty appointment in the Information School and the University of Washington Institute of Technology, Tacoma. She previously held executive positions with The Boeing Company, Seattle, WA, USA. Her current research interests include calibration of low layer network devices, network forensic readiness methodologies, security vulnerabilities in critical infrastructure.

Ms. Endicott-Popovsky is a member of the IEEE, a founding member of the NW Regional Computer Forensics Cooperative, Principal Investigator on numerous grants, producer of the televised Unintended Consequences of the Information Age Lecture series. She has served on organizing committees for the International Workshop on Systematic Approaches to Digital Forensic Engineering and the Recent Advances in Intrusion Detection (RAID) conference and is on

the editorial board of a Special Edition of the Journal on Educational Resources in Computing.

Carol Taylor (Chicago, Illinois) She has her PhD and Masters of Science in Computer Science from the University of Idaho, USA (2001, 2004), and a BS in Computer Science from Colorado State University, USA (1985).

She is a post-doctoral researcher at the University of Idaho and an Assistant Professor at Eastern Washington University, Cheney, Washington, USA. She has over 12 years of computer industry experience, having worked in both industry and government as a software developer and systems analyst. She has conducted research in the areas of intrusion detection, formal methods and digital forensics and examined layered certification of software components using the DOD Common Criteria. Her current research interests include computer security and information assurance with special interests in formal methods, trustworthy systems, intrusion detection and digital forensics.

Dr. Taylor is a member of the ACM, AWIS, AAUW, IEEE, and is actively involved in the CS education community.

Deborah Frincke (Champaign, Illinois) She has her Ph.D. and Masters of Science in computer science from the University of California, Davis, Davis, CA, USA (1989, 1992), and a BS in Mathematics and Computer Science from the University of California, Davis, Davis, CA, USA (1985).

She is Chief Scientist for CyberSecurity Research in the Computational Sciences Directorate at the Pacific Northwest National Laboratory, Richland, Washington, USA. She has been a faculty member at the University of Idaho, Moscow, Idaho, USA, from 1993-2007, achieving the rank of Full Professor. She co-founded TriGeo Network Security in 1999, based on her early University of Idaho research. Her current research interests include very large system defense, forensics, infrastructure protection, security visualizations, SCADA security, and computer security education.

Dr. Frincke is a member of the ACM, AWIS, IEEE, ISOC and was one of the founding members of the Colloquium for Information Systems Security Education .She has been Principal Investigator on numerous grants and a member of governing boards at the University of Idaho. She has been program chair for the International Workshop on Systematic Approaches to Digital Forensic Engineering and the Recent Advances in Intrusion Detection (RAID). She is a member of the editorial board for *IEEE Security and Privacy* and serves on the editorial boards of *International Journal of Information and Computer Security, Journal of Computer Security* and the *Journal of Computer Networks*.