available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

Specifying digital forensics: A forensics policy approach

Carol Taylor[a,*], Barbara Endicott-Popovsky[b,1], Deborah A. Frincke[c]

[a]University of Idaho, Computer Science Department, Moscow, ID 83844, United States
[b]Center of Information Assurance and Cybersecurity, Box 354985, University of Washington, Seattle, WA 98105, United States
[c]Pacific Northwest National Laboratory, Richland, WA 99352, United States

Keywords:
Digital forensics
Policy
Computer security
System specification
Forensic properties

ABSTRACT

In this paper we present an approach to digital forensics specification based on forensic policy definition. Our methodology borrows from computer security policy specification, which has accumulated a significant body of research over the past 30 years. We first define the process of specifying forensics properties through a forensics policy and then present an example application of the process. This approach lends itself to formal policy specification and verification, which would allow for more clarity and less ambiguity in the specification process.

1. Introduction

Digital forensics is an emerging area within the broader domain of computer security whose main focus is the discovery and preservation of digital evidence for proof of criminal wrongdoing and ultimate prosecution of criminal activity (Endicott-Popovsky and Frincke, 2006). Computer evidence is becoming a routine part of criminal cases with nearly 85% of the current caseloads involving digital evidence (Meadaris, 2006).

Yet, for all its growing importance, digital forensics practice is often *ad hoc* and generally lacking in widely accepted theoretical models or principles. Unlike computer security, which defines security properties such as confidentiality, integrity and availability as its three major characteristics, a similar set of properties for digital forensics does not currently exist.

If computer forensics properties have yet to be defined, then there is no standard way to specify an IT system's forensics capabilities or to formally compare systems.[2] Consequently, there is no recognized means to implement mechanisms that enforce forensics capability.

As this field matures, advances need to be made in how forensics capabilities are specified, implemented and verified. Standardized properties need to be defined and acknowledged by the forensics community so that agreement can be reached on methods for implementation and formal proof that systems meet these properties.

One exception to the lack of agreed upon forensics properties is forensic readiness, the ability of a system to efficiently capture and use digital evidence. Yet, while forensic readiness is somewhat supported within the digital forensics research community (Endicott-Popovsky and Frincke, 2006; Tan, 2001; Yasinsac and Manzano, 2001), the specification and implementation of this property are not consistent within the digital forensics community (Endicott-Popovsky and Frincke, 2006).

There are potential benefits from creating better methods for forensics specification. A primary benefit of more clearly specified forensics requirements is that systems can then be designed to meet these requirements. Another advantage to creating a standardized, precise, repeatable means of defining digital forensics characteristics is the potential for defining

* *Corresponding author.*
E-mail addresses: ctaylor@cs.uidaho.edu (C. Taylor), endicott@u.washington.edu (B. Endicott-Popovsky), deborah.frincke@pnl.gov (D.A. Frincke).
[1] Tel.: +1 206 284 6123; fax: +1 206 216 0537.
[2] For our purposes, we define a system as an IT or enterprise system, taking the view of the first responders to an incident response.
1742-2876/$ – see front matter
doi:10.1016/j.diin.2007.06.006

more universal forensics properties. Having widely acknowledged, properties for systems that capture digital data would assist everyone including law enforcement, system implementers, and system administrators in understanding forensics requirements and the limits of systems in satisfying the requirements.

In this paper we propose a method for specifying forensics systems properties with an approach borrowed from the computer security domain. Computer security is typically defined according to a security policy, which "is a statement of what is, and is not, allowed" by the system (Bishop, 2004). Once there is a clear statement of permissible and non-permissible behavior for a system, security enforcement mechanisms can be implemented to uphold the policy. Computer forensics capability can be similarly specified according to a forensics policy, which would define details of "capturability" for specific resources or events of interest. Forensics policy enforcement mechanisms in the form of devices or procedures could then be specified in support of the policy. While the goals of security and forensics policies differ, the mechanisms of specification and enforcement are similar.

There are several advantages to using a forensics policy approach in order to specify forensics capability for a system. One advantage is that there is a large body of security policy research, which can be borrowed from and applied to the digital forensics problem (Bishop, 2004). Another benefit to clearly defining a forensics policy is the ability to unambiguously specify system capacity in order to meet the policy (Tan, 2001). Along these same lines, formalizing the policy would further clarify the capabilities needed to meet the policy and allow for formal verification of the forensics capabilities of the system.

This short paper is organized into five sections. It is not intended to present definitive forensics policies, but rather to encourage further exploration of the subject by offering an exemplar policy to show how one might be implemented. This section introduced the problem of forensic capability definition. Section 2 introduces the property of forensic readiness, which will be used to illustrate our policy-based approach. Section 3 presents our forensics policy approach to forensics system specification. In Section 4, we demonstrate a policy approach to defining forensic readiness. Section 5 concludes the paper and outlines our future work.

2. Forensic readiness

The concept of forensic readiness for a system describes the capability of the system to efficiently collect credible digital evidence that can then be used in legal proceedings. Efficiency for digital forensics has been described in terms of cost since costs tend to be significant especially for systems that are not forensics ready. Credible digital evidence refers to data that have been collected and preserved through a process that does not invalidate the legitimacy of the data.

Forensic readiness is one of the few proposed forensics characteristics discussed in the forensics literature. Forensic readiness was proposed by Tan (2001) in order to meet two objectives for systems used in digital investigations: (1) costs should be minimized for incident responses and (2) an environment's ability to collect digital evidence should be maximized. In his original paper on forensic readiness, Tan described many specific techniques for achieving digital forensic readiness including logging techniques, IDS data usage, forensic acquisition and evidence handling.

A later paper describes how forensic readiness can be built into an enterprise forensics program and outlines 10 steps to achieving forensic readiness (Rowlinson, 2004). The main point of this paper is that forensic readiness makes sense from a business perspective and can result in cost savings should there be an investigation. Enterprises should be actively collecting potential evidence such as log files, network traffic records, e-mail and telephone records prior to involvement in an investigation (Rowlinson, 2004).

Others described different aspects of system forensic readiness including policies for enhancing digital forensic readiness (Yasinsac and Manzano, 2001), incorporation into existing response plans (Wolfe-Wilson and Wolfe, 2003) and making sure forensic readiness leads to sound investigation (Carrier and Spafford, 2003). Another perspective discusses ensuring that hardware devices used to capture forensic evidence are reliable enough to enforce forensic readiness (Endicott-Popovsky and Frincke, 2006). As the wide divergence of these studies illustrate, there is no one methodology or approach to enabling forensic readiness within a system or enterprise.

3. Forensic policy approach

In this section we present our approach to defining forensics capabilities for a system based on concepts from computer security policy research. We note that while the risks to systems for computer security and forensics differ, the process of specification and enforcement of the policies are similar. We present background on how security policies are defined and help support system security and then show that the same approach will benefit forensic property definition.

3.1. *Security policy specification*

A security policy is a statement that clearly specifies what is allowed and what is disallowed with regards to security. At the lowest level security policies partition the states of a system into a set of authorized or secure states and unauthorized or insecure states (Bishop, 2004). Essentially, one can view a security policy as a set of statements that when enforced result in a secure system. The statements themselves are the security requirements for the system that must be met or enforced so that system behavior results in only authorized states (Bishop, 2004).

Another way to view security policies is as a description of security goals for a system and how a system should behave to meet the goals. Since security goals for a system affect how security mechanisms on the system are configured, security policies should be stated clearly (Clark and Wilson, 1987).

A well-known example of a security policy for a military system deals with confidentiality of classified data. A high-level security goal for this type of system is that the system should prevent unauthorized disclosure or theft of

information (Clark and Wilson, 1987). The corresponding military security policy states that all classified information shall be protected from unauthorized disclosure or declassification. Enforcement mechanisms include mandatory labeling of all documents with their classification level and assignment of user access categories based on a person's authorization or clearance (Clark and Wilson, 1987). Enforcement is also mandatory so that everyone dealing with classified data must follow these rules.

3.2. *Forensic policy specification*

Digital forensics seeks to capture digital evidence such that the forensic integrity of the data is preserved for legal purposes. Consequently, forensic policies must address the requirement for both capture and preservation of evidence.

A forensics policy should clearly state the forensics functionality of a system. Thus, instead of specifying what is allowed and not allowed, a forensics policy will specify the events that must be handled and data surrounding the events that must be preserved. Events not included in this list will not be forensics noteworthy and data for these incidents will not need to be preserved for forensics reasons. Consequently, a forensics policy partitions the space of all possible breaches or criminal activity into a set of events, which require forensic action, and those that do not.

An example of a very simple forensics policy for a commercial system addresses security breaches for the network. One forensics goal is to preserve data from actual intrusions or security violations. The policy for this commercial system states that all events identified as intrusions or potential intrusions on the network will have their associated data captured and preserved in the event that prosecution is sought. Enforcement mechanisms for this policy include routine preservation of IDS, firewall and router logs plus web server logs for the public web server. Logs will be archived and stored for a configurable amount of time. Network capacity will be maintained at a level sufficient to guarantee that packets are not routinely dropped so that data integrity due to packet loss will not be a concern.

4. Forensics policy for forensic readiness

This section describes how requirements for forensic readiness can be specified using the forensics policy approach discussed in the previous section.

4.1. *Determining forensic readiness requirements*

Forensic readiness, as described in Section 2, attempts to maximize the usefulness of digital data gathered with the least amount of cost. Consequently, systems that prepare for potential legal incidents by collecting and preserving data can actually reduce costs of later prosecutions (Rowlinson, 2004).

Examining the requirements for forensic ready systems without a clear statement of the events of interest would result in a perhaps incomplete specification or an overzealous and inefficient use of resources by attempting to preserve everything. Criminal actions that should have been prosecuted might not have the associated data saved to determine guilt, or the lack of separating the events of interest could result in having to record and save a great deal of unnecessary data. A clearly stated forensics policy would greatly clarify what needs to be preserved and for which set of events.

Forensics Policy

1. All access to Oracle DB must be monitored.
2. Access logs and Administration logs to Oracle DB will be preserved for no less than one year
3. Access and activity to Web server is monitored
4. Apache Web server logs will be preserved for 6 months
5. Firewall and Snort logs will be preserved for one year
6. Router logs will be preserved for 6 months
7. Network will be tested every 6 months for congestion situation by overloading it until it begins to drop traffic
8. Network capacity will be increased before traffic hits the level where packets will be dropped

Fig. 1 – Forensics policy for a corporate IT system.

So, how does one define a forensics policy addressing forensic readiness for a given system? The following process assists in defining a forensics policy that addresses forensic readiness requirements:

- Identify digital assets that have value.
- Perform a risk assessment for potential loss and threat to those assets.
- Remove assets that do not warrant the effort of prosecution.
- Identify associated data needed for these assets along with collection and storage needs.
- Write the forensic policy in terms of digital assets, forensic events, data collection and storage.
- Ensure adequate forensics policy enforcement is in place.

Fig. 1 outlines a hypothetical forensics policy developed for a hypothetical corporate system containing a high value Oracle database, a less valuable public Apache web server (but one still worth prosecuting if it is breeched), CISCO network routers, several firewalls and a Snort IDS system. It was derived using the suggested process outlined previously and is an example of a security policy.

5. Conclusions and future work

In this paper we introduced an alternative approach for specifying and defining forensics capabilities or properties for an IT system based on a forensics policy. The concept is borrowed from the security community, which traditionally relies on security policies for specifying the security of a system and the enforcement mechanisms that uphold the security policy. But while security policies divide a system into

sets of authorized and unauthorized states, forensic policies separate the events and associated data worthy of legal action from those events that would not ever be prosecuted.

We demonstrated the approach by defining a forensics policy for the property of forensic readiness, one of the few proposed forensics properties described in the literature. Forensic policies for forensic readiness should address the data needed to support prosecution of criminal acts associated with certain assets as opposed to preserving data associated with all assets. The latter case could prove wasteful and costly.

In this paper, forensics policies were stated informally, which can lead to ambiguity in specifying enforcement mechanisms in addition to potential inconsistencies within the policies themselves. Consequently our future work will explore formalizing the forensics policies in order to add preciseness and eliminate potential fuzziness in policy definition.

Other advantages of formal policy specification include being able to prove that a policy is correct, being able to reason about system properties and discovering incomplete specifications prior to implementation (Bishop, 2004).

Formal forensics policy specification does not guarantee correctness in implementation since systems are still constructed manually; however, the formal process has the advantage of being precise and potentially verified so that the manual development effort proceeds from a correct specification.

Our ultimate goal in relying on a forensic policy, both informal and formal, is that forensics capability will be designed-in or added-on in the form of forensics enforcement mechanisms so that systems will be better equipped to capture and correctly preserve digital evidence.

REFERENCES

Bishop M. Introduction to computer security. Addison-Wesley; 2004.

Carrier B, Spafford E. Getting physical with the digital investigation process. Int J Digit Evid Fall 2003;2(2).

Clark DD, Wilson DR. A comparison of commercial and military computer security policies. In: Proceedings of the IEEE symposium on security and privacy, 1987. p. 184–919.

Endicott-Popovsky B, Frincke D. Embedding forensic capabilities into networks: addressing inefficiencies in digital forensics investigations. In: Proceedings of the 2006 IEEE workshop on information assurance: computer forensics. West Point, NY: United States Military Academy; June 2006.

Meadaris K. Grants to help develop ways to improve digital evidence collection. Purdue University, <http://www.purdue.edu/UNS/html4ever/2006/061012RogersGrant.html>; October 2006.

Rowlinson R. Ten steps to forensic readiness. Int J Digit Evid Winter 2004;2(3).

Tan J. Forensic readiness. Cambridge, MA: Stake; 2001.

Wolfe-Wilson J, Wolfe HB. Management strategies for implementing forensic security measure. Inform Secur Tech Rep June 2003;8(2):55–64.

Yasinsac A, Manzano Y. Policies to enhance computer and network forensics. In: Proceedings of the 2001 IEEE workshop on information assurance and security. West Point, NY: United States Military Academy; Jun 2001.

Carol Taylor, Ph.D. in Computer Science, University of Idaho (2004), is a post-doctoral researcher at the University of Idaho and Assistant Professor at Eastern Washington University. She has conducted research in the areas of computer security and information assurance with special interests in intrusion detection, formal methods and digital forensics and layered certification of software components using the Common Criteria. Her current research interests include formal methods applied to digital forensics, trustworthy systems, and intrusion detection.

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

Barbara Endicott-Popovsky, Ph.D. candidate Computer Science, University of Idaho (Summer 2007), is the Director of the Center for Information Assurance and Cybersecurity at the University of Washington with a joint faculty appointment in the Information School and the University of Washington Institute of Technology, Tacoma. Her current research interests include calibration of low layer network devices, network forensic readiness methodologies, security vulnerabilities in critical infrastructure.

Endicott-Popovsky is a member of the IEEE, a founding member of the NW Regional Computer Forensics Cooperative, and a member of the organizing committees for the International Workshop on Systematic Approaches to Digital Forensic Engineering and the Recent Advances in Intrusion Detection (RAID) conference.

Deborah Frincke, Ph.D. University of California, Davis, 1992, is Chief Scientist for CyberSecurity Research in the Computational Sciences Directorate at the Pacific Northwest National Laboratory. She has been a faculty member at the University of Idaho, from 1993 to 2007, achieving the rank of Full Professor. Her current research interests include very large system defense, forensics, infrastructure protection, security visualizations, SCADA security, and computer security education.

Frincke is a member of the ACM, AWIS, IEEE, ISOC and is a member of the editorial board for *IEEE Security and Privacy*, *International Journal of Information and Computer Security*, *Journal of Computer Security* and the *Journal of Computer Networks*.