An Investigative Framework for Incident Analysis

Clive Blackwell

Chapter 2

AN INVESTIGATIVE FRAMEWORK FOR INCIDENT ANALYSIS

Clive Blackwell

Abstract A computer incident occurs in a larger context than just a computer network. Because of this, investigators need a holistic forensic framework to analyze incidents in their entire context. This paper presents a framework that organizes incidents into social, logical and physical levels in order to analyze them in their entirety (including the human and physical factors) rather than from a purely technical viewpoint. The framework applies the six investigative questions – who, what, why, when, where and how – to the individual stages of an incident as well as to the entire incident. The utility of the framework is demonstrated using an insider threat case study, which shows where the evidence may be found in order to conduct a successful investigation.

Keywords: Incident framework, security architecture, investigative questions

1. Introduction

Security incident ontologies often provide subjective and incomplete representations of incidents by focusing on the digital aspects and only considering the offensive or defensive viewpoints. They do not include the interactions between people and their external physical and digital environments. These interactions provide a wider investigative context for the examination of the progression and effects of incidents.

The utility of these models to digital forensics is also unclear because they do not elucidate the evidence available to the investigator after the event or map to investigative goals. It is necessary to model the investigator's methods, tools and techniques in evidence collection, analysis and response to meet the goals of incident discovery, attribution, recovery, fixing weaknesses and prosecution.

Table 1. Zachman framework.

	Why	**How**	**What**	**Who**	**Where**	**When**
Contextual	Goal list	Process list	Material list	Org. unit and role list	Geog. location list	Event list
Conceptual	Goal relationship	Process model	ER model	Org. unit and role model	Location model	Event model
Logical	Rule diagram	Process diagram	Data model diagram	Role diagram	Location diagram	Event diagram
Physical	Rule spec.	Process functional spec.	Data entity spec.	Role spec.	Location spec.	Event spec.
Detailed	Rule details	Process details	Data details	Role details	Location details	Event details

This paper presents a digital forensic investigative framework that considers computer crime and incidents in their entirety rather than as logical incidents alone. The framework incorporates three layers that comprise the social, logical and physical levels of an incident; it extends and adapts the Zachman framework [16] and the Howard-Longstaff security incident taxonomy [5]. Each layer consists of several sublevels for more detailed analysis, two for the physical and social levels, and five for the logical level. The resulting framework presents a holistic and persuasive forensic analysis, which considers the entire incident context (including human and physical factors) to observe, analyze and prove incident causality.

The framework also facilitates the decomposition of complex incidents into their atomic stages along with their causes and effects. This is crucial because evidence about incident events and their timeline may be partial and indirect after the incident, requiring the investigator to infer the missing events from hypotheses about the incident. The utility of the investigative framework is demonstrated using a case study involving the insider threat.

2. Background

The Zachman framework [16] (Table 1) is a complex model for designing enterprise computing architectures. This framework attempts to capture and organize information about every aspect of an organization related to its computing requirements. It consists of five levels: contextual, conceptual, logical, physical and detailed. The Zachman framework

also provides a second dimension where six questions are posed to describe the different aspects of the system; these questions are answered for each of the five levels.

Unlike the Zachman framework, the proposed forensic framework is intended to guide the investigative process and establish the completeness of incident analysis. Since the focus is on modeling processes and not on designing enterprise computing architectures, the investigative questions in the Zachman framework are adapted to operational concerns.

Ieong [6] has adapted the Zachman framework for forensic analysis in the FORZA framework. The FORZA questions are analogous to the Zachman questions, except that they are applied to operational concerns. The investigative framework presented in this paper differs from FORZA by posing all six questions for each stage in an incident progression as well as for the entire incident. Interestingly, the U.S. Department of Justice's Digital Forensics Analysis Methodology [15] asks five of the six questions (omitting why) in the analysis phase. Pollitt [10] has analyzed the investigative process, which is distinct from the incident process discussed in this work.

The Sherwood Applied Business Security Architecture (SABSA) [13] is an adaptation of the Zachman framework to security. SABSA considers each of Zachman's concepts from a security perspective, replacing each cell in the table with its security analog.

Howard and Longstaff [5] have proposed an alternative security incident taxonomy (Figure 1). The Howard-Longstaff taxonomy organizes incidents into stages with different purposes, actors, scopes and effects. The categories are attacker, tool, vulnerability, action, target, unauthorized result and objectives. The attacker uses a tool to perform an action that exploits a vulnerability on a target, causing an unauthorized result that meets the attacker's objectives.

3. Digital Forensic Framework

The proposed digital forensic investigative framework focuses on the social, physical and logical aspects of incidents. It extends the Zachman framework [16] and the Howard-Longstaff taxonomy [5]. The extension enables the investigative framework to support detailed and comprehensive analyses of incidents.

The proposed framework comprises three layers: social, logical and physical. Each layer is partitioned into sublevels to support more detailed analyses. The resulting partitioning follows the OSI seven-layer

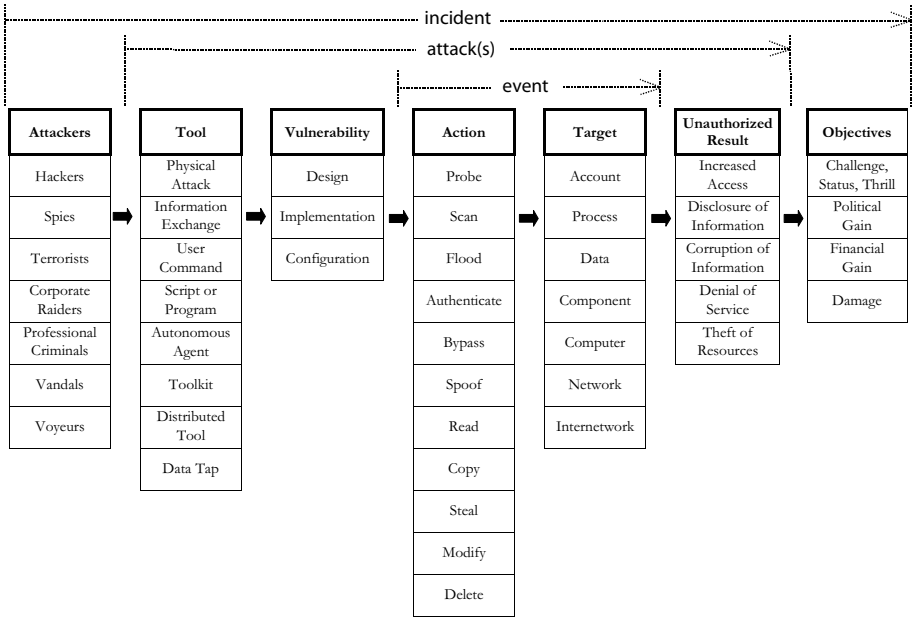

Figure 1. Howard-Longstaff security incident taxonomy [5].

model [14]; it has two sublevels for the social and physical layers, and five for the logical layer.

The Zachman framework and the Howard-Longstaff taxonomy do not address the possibility that a perpetrator may use a third party to perform a stage of the incident. This can take the form of social engineering or using an intermediary computer or user account at the logical level. For this reason, we separate an incident into two components. The first component is the complete incident containing the perpetrator's objective or ultimate goal. The second is the stage, which contains the specific details of the event and contains most of the evidence.

3.1 Social Level

The social level of the investigative framework covers incident perpetrators and their intangible attributes such as motivation. It permits the differentiation between real-world actions and the resulting effects on people and organizations.

The social level consists of the reflective and activity sublevels, which contain intangible aspects such as motivation, and tangible concerns such as actions and their effects respectively (modeled in Figure 2). With regard to the investigative questions, the reflective sublevel includes the

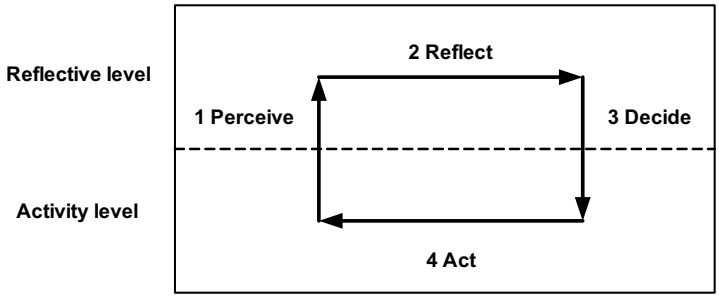

Figure 2. Duality of thoughts and actions in the investigative process.

motivation (ultimate why) and abilities (latent aspect of the ultimate how) of the perpetrator. The involved people and organizations (ultimate who) occupy the entire social level, encompassing both sublevels to represent the duality of their thoughts at the reflective sublevel and actions at the activity sublevel.

The reflective sublevel contains the evidence relevant to the investigation that is lifted from information collected in the lower levels. The evidence seeks to answer the who, what, why, when, where and how questions about each individual stage of an incident as well as about the entire incident. The proposed framework assists by specifying where and when this evidence can be collected.

The activity sublevel, which occupies the remainder of the social level, relates to incident progression and investigative processes that involve action. It contains the abstraction of the resources and authority (remainder of the ultimate how) of the involved parties. The how is performed at the lower levels, but the progression of the entire incident and corresponding investigation can be modeled conceptually at the social level by abstracting its low-level execution. The objectives (ultimate what) are at the activity sublevel if their intent is to bring about a financial or functional gain. They are at the reflective sublevel if they are psychologically motivated (e.g., revenge by a disgruntled employee).

The ultimate when and ultimate where relate to the conceptual locations where the lower-level actions affect people and organizations at the social level. A victim of credit card fraud is affected if the card is declined (ultimate when) while making a purchase (ultimate where). The actual incident occurs at the lower levels, such as the logical level if the credit card details were stolen and used to make unauthorized purchases. The logical effects of reducing the available funds in the cardholder account database are latent in nature and do not directly affect the victim. The victim is only affected when he/she attempts to use the funds later,

which occurs at the social level by reducing his/her ability to purchase goods.

3.2 Logical Level

The logical level has five sublevels: application, service, operating system, hardware and physical.

The application sublevel deals with logical services and the use of logical resources such as data. At this sublevel, an incident has a logical effect through undesirable events or changes in the logical state (logical what); this is because the application sublevel meets the social level objectives. The incident actions (logical how) occur at lower levels that are controlled by the operating system. For example, credit card use is at the application sublevel when purchases are made online while its computational operations are executed at lower levels. The investigator needs to establish the link to a person via the social-logical interface based on the logical activities carried out on the person's behalf. The user is the logical agent (logical who) that executes logical processes at the lower levels. The purpose of logical actions (logical why) is derived from their ultimate purpose at the social level.

The service sublevel provides methods (logical how) for obtaining the results required by an application (logical why) through some processing, communication, translation, storage or protection service. In general, the lower logical sublevels provide methods (logical how) for obtaining the results required by the higher levels (logical why); thus, the how at each upper level becomes a why when it is performed at a lower level.

Logical operations are executed in a low-level venue (logical where and when). The investigator may find potential evidence at the lower levels from residual data after its higher-level representation has been destroyed. However, specialized expertise and tools are often needed to recover the data because the lower levels are not intended to be directly accessible. In addition, the investigator may face significant challenges in interpreting the collected data as evidence because low-level events are far removed from the ultimate cause.

3.3 Physical Level

The physical level is also significant with regard to computer incidents. This is because many incidents combine the logical and physical aspects, and all computational activities are ultimately performed at the physical level.

The physical level contains two sublevels: the material sublevel of substantial objects and the wave sublevel of intangible phenomena (e.g.,

Table 2. Investigative framework for sabotage incidents by disgruntled employees.

Incident Entity	**Perpetrator**	**Method**	**Ultimate Effect**	**Incident Objectives**	**Ultimate Target**
Investig. Questions	**Ultimate Who**	**Ultimate How**	**Ultimate What**	**Ultimate Why**	**Ultimate Where**
Social Level	Disgruntled employee	Social engineering; Existing or illegal access	Revenue loss; Customer loss	Revenge	Employee's organization

electromagnetic radiation) that are determined by the size of the object and the focus of the investigation. The material sublevel covers the physical aspects of a crime scene investigation that involves long-established techniques.

The physical level is significant for incidents that involve computational and physical actions, in which case there needs to be comprehensive collection and integration of evidence at all levels. An example is the Integrated Digital Investigation Process (IDIP) [3], which unifies digital and physical crime scene investigations. All activities are ultimately executed physically, so the six investigative questions can be asked about the execution of any higher-level process at the physical level.

4. Operational Framework

The incorporation of the Zachman framework [16] and the Howard-Longstaff [5] taxonomy is an important aspect of the framework. The ultimate and stage components are decomposed into the six investigative questions from the Zachman framework (who, what, why, when, where and how). The ultimate and stage investigative questions map to the Howard-Longstaff model, where the who refers to the attackers, the how is the method/tool and the vulnerability, the why is the reasons/objectives, the where is the target, and the what is the effect and the unauthorized result. The when is included implicitly in the proposed framework table within the timeline of incident progression. Table 2 presents the framework for an insider threat involving sabotage. Table 3 shows the associated stage aspects.

The incident classification is linked with the six investigative questions to help organize the investigation. Tables 2 and 3 have headings for the incident and stage entities, processes, purposes and outcomes, respectively, along with the investigative questions (five of the questions are subheadings of an incident column and a stage column). It is necessary to raise the information collected about incident events to the status of

Table 3. Stage aspects for sabotage incidents by disgruntled employees.

Stage Entity	**Actor or Agent**	**Reason**	**Action**	**Target**	**Unauth. Result**
Investig. Questions	**Stage Who**	**Stage Why**	**Stage How**	**Stage Where**	**Stage What**
Social Level	Perpetrator; Employee acting for perpetrator	Persuade others to act; Avoid responsibility; Gain access to resource	Persuade, trick, bribe, threaten; Exploit trust	Security guard; System administrator; Colleague	Increase access; Employee action on behalf of perpetrator
Logical Level	Own account; Compromised account; Malware	Gain privileged access to interfere with systems and avoid accountability	Illegal access; Exploit weakness; Install malware; Misuse privilege	Business process; Account data; Application program; Operating system; Computer; Network	Damage system integrity; Deny resources and services
Physical Level	Physical perpetrator; Manipulated employee	Gain physical access to facilities, equipment, computers for theft or to cause damage	Trick guard, steal or borrow keys; Theft; Damage or destroy equipment	People; Computer; Network; Data; Equipment	Personal injury; Computer, network or data theft or damage

evidence at the social level, which requires reasoned, relevant and admissible arguments. The steps at the lower levels of the stage table may be annotated with vertical arrows to show how the investigation can transform collected information about the contents of each column to evidence at the social level by answering the corresponding investigative question. The responses to the stage questions help answer the incident questions, where the stage answers regarding low-level isolated events have to be connected to the incident answers about the overall incident causes and effects at the social level.

5. Insider Threat from Sabotage

A CERT survey [2] has identified that disgruntled employees cause a significant proportion of sabotage after they are terminated. Tables 2 and 3 show some of the possible incidents of sabotage by a disgruntled employee. For example, the perpetrator's actions could be tricking a colleague (social ultimate how) into giving out his/her password (social

stage how), which allows the colleague's account to be misused (logical ultimate how) to damage the file system (logical stage how) so that data is lost and services cannot be provided (logical stage what).

The main points of the proposed digital forensic investigative framework are:

- The progressive nature of stages from system access to target use to incident outcome.
- The ultimate effects of an incident are social, but the stage actions are performed at lower levels. This requires an adequate amount of reliable evidence to prove the connection between the actions and the perpetrator.
- Different stage actors have different motivations (e.g., a system administrator and a colleague who has been tricked into giving unauthorized access).
- The ultimate objective for the perpetrator may be psychological, but tangible damage is caused to the victim, showing the need for separate analysis of the effects on both parties and the relationship between them.
- Indirect evidence can be collected at different locations, levels or stages, occupying different cells in a table from the causative action.
- The lower logical and physical levels may not be directly used by the perpetrator, but are important in investigating when the higher-level primary evidence was destroyed.

6. Investigative Process

The utility of many incident models to digital forensics is unclear because they do not elucidate the possible evidence available to an investigator after the event, nor do they map incident data to the investigative goals. The proposed investigative framework considers incidents within a wider context and from multiple perspectives to facilitate broader and deeper investigations. The focus extends beyond computer misuse to the wider social, organizational, legal and physical contexts.

Key advantages of the framework include the clarification of the spatial and temporal scope of the different investigative stages, the iteration of and feedback between stages, and the introduction of an additional stage involving remedial actions to improve the investigative process.

The proposed investigative framework also provides a metamodel for representing other digital forensic frameworks [1, 3, 4, 8, 9, 11]. As an example, the mapping by Selamat, *et al.* [12] has five stages of incident investigation: preparation, collection and preservation, examination and analysis, presentation and reporting, and dissemination. The proposed incident model has three main active stages of access, use and outcome that map to the middle three stages of the model of Selamat and colleagues when considered from the point of view of the investigator. The incident access stage obtains greater system and resource control for the perpetrator, whereas the investigator's collection and preservation phase discovers and controls the evidence. The incident use stage performs activities on or with the target resource, analogous to the investigator's examination of the collected evidence. The incident outcome stage corresponds to the presenting and reporting stage. The incident may also have a preparatory stage that reconnoiters the target, which maps to the investigation preparation stage. Also, there are often further actions after the active incident (e.g., use or sale of the targeted resource) that correspond to the final investigation dissemination stage. Therefore, the investigative framework becomes similar to Selamat and colleagues' approach, when the investigative process is modeled analogously to incident progression.

The proposed dual investigative process is nearly symmetrical to the incident progression in terms of its structure. However, it is important to take into account the incomplete and possibly incorrect information available to the investigator, because of the discrepancy between the observation of offensive events and the information that is available later for their detection and remediation. Provision must also be made for secondary observations and inferences about past events when the primary evidence has been destroyed or has not been collected.

The investigative process is connected to incident events using an adaptation of the scientific method involving observation, hypothesis, decision and action [7]. In the scientific method, the prediction of physical events is based on the fundamental assumption of the uniformity and pervasiveness of the laws of nature. The physical world is not malicious and does not deceive observers with fake measurements. However, the perpetrator could have altered the appearance of events so that they are undetectable, appear normal or have legitimate causes. These activities may be determined by secondary evidence from side effects of the incident or via system monitoring activities such as analyzing audit logs. It is important to note that any system that has been penetrated cannot be trusted. Unfortunately, dealing with this problem in a comprehensive manner appears to be intractable at this time.

7. Conclusions

The digital forensic investigative framework presented in this paper organizes incidents into the social, logical and physical levels, and applies Zachman's six investigative questions to the incident and its stages. The framework allows incident progression to be analyzed more completely and accurately to meet the investigative goals of recovery and accountability. The application of the framework to an insider threat case study demonstrates how information about incident events can be transformed into evidence at the social level using sound investigative processes.

References

[1] N. Beebe and J. Clark, A hierarchical, objectives-based framework for the digital investigations process, *Digital Investigation*, vol. 2(2), pp. 147–167, 2005.

[2] D. Cappelli, A. Moore, R. Trzeciak and T. Shimeall, Common Sense Guide to Prevention and Detection of Insider Threats, Version 3.1, CERT, Software Engineering Institute, Carnegie-Mellon University, Pittsburgh, Pennsylvania, 2009.

[3] B. Carrier and E. Spafford, Getting physical with the digital investigation process, *International Journal of Digital Evidence*, vol. 2(2), 2003.

[4] B. Carrier and E. Spafford, An event-based digital forensic investigation framework, *Proceedings of the Fourth Digital Forensics Research Workshop*, 2004.

[5] J. Howard and T. Longstaff, A Common Language for Computer Security Incidents, Sandia Report SAND98-8667, Sandia National Laboratories, Albuquerque, New Mexico and Livermore, California, 1998.

[6] R. Ieong, FORZA: Digital forensics investigation framework that incorporates legal issues, *Digital Investigation*, vol. 3(S1), pp. 29–36, 2006.

[7] W. McComas, The principal elements of the nature of science: Dispelling the myths in the nature of science, in *The Nature of Science in Science Education*, W. McComas (Ed.), Kluwer, Dordrecht, The Netherlands, pp. 53–70, 1998.

[8] G. Palmer, A Road Map for Digital Forensic Research, DFRWS Technical Report DTR – T001-01 Final, Air Force Research Laboratory, Rome, New York (dfrws.org/2001/dfrws-rm-final.pdf), 2001.

[9] M. Pollitt, Computer forensics: An approach to evidence in cyberspace, *Proceedings of the National Information Systems Security Conference*, pp. 487–491, 1995.

[10] M. Pollitt, Six blind men from Indostan, *Proceedings of the Fourth Digital Forensics Research Workshop*, 2004.

[11] M. Reith, C. Carr and G. Gunsch, An examination of digital forensic models, *International Journal of Digital Evidence*, vol. 1(3), 2002.

[12] S. Selamat, R. Yusof and S. Sahib, Mapping process of digital forensic investigation framework, *International Journal of Computer Science and Network Security*, vol. 8(10), pp. 163–169, 2008.

[13] J. Sherwood, A. Clark and D. Lynas, *Enterprise Security Architecture: A Business Driven Approach*, CMP Books, San Francisco, California, 2005.

[14] A. Tanenbaum, *Computer Networks*, Prentice-Hall, Upper Saddle River, New Jersey, 2003.

[15] U.S. Department of Justice, Digital Forensics Analysis Methodology, Washington, DC (www.justice.gov/criminal/cybercrime/forensics_chart.pdf), 2007.

[16] J. Zachman, A framework for information systems architecture, *IBM Systems Journal*, vol. 26(3), pp. 276–292, 1987.