Network Forensics Models for Converged Architectures

Juan C. Pelaez
U.S. Army Research Laboratory
APG, MD 21005, USA
juan.c.pelaez@arl.army.mil,

Eduardo B. Fernandez
Department of Computer Science and Engineering
Florida Atlantic University
Boca Raton, FL 33433, USA
ed@cse.fau.edu

Abstract— We discuss a systematic approach to network forensic collection and analysis of data in converged networks. Since attacks cannot be completely avoided, it is necessary to have appropriate forensics systems. Upon integration into a network forensic infrastructure, we expect this forensic model will enable a faster response and more structured investigations of Voice over IP (VoIP)-based network attacks.

Keywords—forensic patterns, network architecture, software architecture, Voice over IP.

I. INTRODUCTION

The generic solutions for problems that occur in similar ways in different contexts or environments can be expressed as patterns. A pattern is an encapsulated solution to a problem in a given context and can be used to guide the design or evaluation of systems [Gam94]. Analysis, design, and architectural patterns are well established and have proved their value in helping to produce good quality software. Recently, security patterns have joined this group and they are becoming accepted by industry [Sch06].

In a recent paper we introduced the concept of attack (i.e., misuse) patterns [Fer07a]. Attack patterns are a systematic description of the steps and objectives of an attack. This type of pattern describes, from the point of view of the attacker, how an attack is perpetrated and analyzes the ways of stopping the attack, including how to trace the steps of the attacker and what information (evidence) can be obtained at each phase. The pattern also attempts to correlate events with specific parts of the system.

In this paper we propose another type of pattern, the Forensic pattern [Pel09a]. It represents a systematic approach to network forensic collection and analysis of data. We introduce it in terms of VoIP networks. In conducting network forensics investigations in a VoIP environment, the collection of voice packets in real time and the use of automatic mechanisms are fundamental. We expect that forensic patterns will enable a faster response and more structured investigations of network attacks. Attacks on some VoIP applications such as VoIP in Tactical Internet require real-time evaluation and analysis, in contrast to the traditional method used in law enforcement, in which the victim's device is taken off-line after an attack has occurred. These patterns would also be useful for training apprentice forensics technicians about common investigative techniques and tools.

Figure 1 shows the relationships between our forensic patterns and existing security patterns. The patterns presented here are indicated with a double line and those under development with a dash line. The first set of Network Evidence forensic patterns provides abstract methods for collection and analysis of evidence; on the other hand, Tactical Evidence patterns are intended for military use (i.e., Tactical Internet). These forensic patterns will also be applicable to law enforcement and to some degree the relevant industry. The collection of all these patterns can be used to build a VoIP network forensic model.

The only other work we know about the use of patterns in forensics is [Dla09], although other works use UML models to describe forensic aspects, e.g., [Bog07].

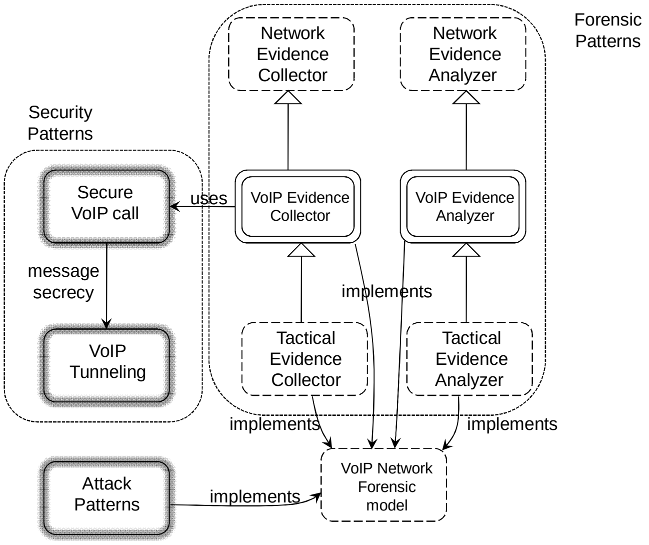
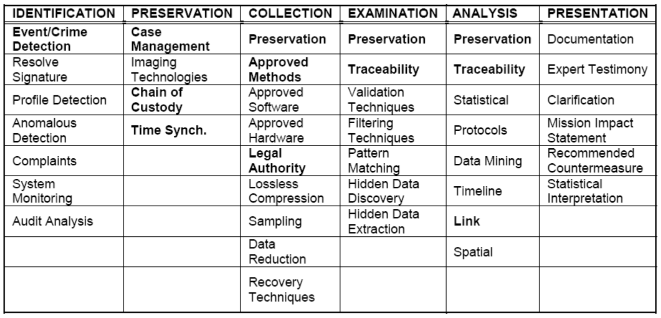


Figure 1 Relationship between VoIP patterns

The rest of the paper is structured as follows. In Section 2 we discuss a Reference Forensic model. In Section 3 we introduce the VoIP Evidence Collector pattern which collects attack packets on the basis of adaptively setting filtering rules of real-time collection. In Section 4 we show the VoIP Evidence Analyzer pattern which analyzes the collected forensics data, and presents a way to investigate and trace back attackers. Section 5 compares our approach to others, while Section 6 presents some conclusions.

II. Reference Forensic Model

Several models are used for investigation in forensic science. We chose the framework from The Digital Forensics Research Workshop (DFRWS) because it is a comprehensive approach and is more oriented to this paper's goals. The DFRWS model shows the sequential steps for digital forensic analysis [DFRWS01]. These steps are shown in Table 1.



IDENTIFICATION	**PRESERVATION**	**COLLECTION**	**EXAMINATION**	**ANALYSIS**	**PRESENTATION**
Event/Crime Detection	**Case Management**	**Preservation**	**Preservation**	**Preservation**	Documentation
Resolve Signature	Imaging Technologies	**Approved Methods**	**Traceability**	**Traceability**	Expert Testimony
Profile Detection	**Chain of Custody**	Approved Software	Validation Techniques	Statistical	Clarification
Anomalous Detection	**Time Synch.**	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement
Complaints		**Legal Authority**	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling	Hidden Data Extraction	**Link**	
		Data Reduction		Spatial	
		Recovery Techniques			

Table 1 - DFRWS Digital Investigative Framework [DFRWS01]

The initial phase or the identification of potential digital evidence (i.e., where might the evidence be found) is covered by Intrusion Detection Systems (IDS) and in some sense by attack patterns, which identify which units of the system have been used in the attack. The Preservation phase involves acquiring, seizing, and securing the digital evidence; making forensic images of the evidence; and establishing the chain of custody. We will concentrate on the middle phases of the forensic process (i.e., the collection, examination and analysis of the evidence) where the presented patterns will provide network investigators an structured method to collect more and better evidence and to reduce the analysis time in VoIP networks.

The presentation phase involves the legal aspects of the forensic investigation – presenting the findings in court and corporate investigative units by applying laws and policies to the expert testimony and securing the admissibility of the evidence and analysis. This phase is outside of the scope of this research, but it must be considered in order to create a comprehensive model.

III. VoIP Evidence Collector

The VoIP Evidence Collector pattern defines a structure and process to collect attack packets on the basis of adaptively setting filtering rules for real-time collection. The collected forensic data is sent to a network forensics analyzer for further analysis. This data is used to discover and reconstruct attacking behaviors.

Context

We are considering a VoIP environment, in which the monitored network should not be aware of the collection process. We assume that evidence is being preserved securely. We also assume a high-speed network with an authentication mechanism and secure transport channel between forensic components.

Problem

How to efficiently collect digital attack evidence in real-time from a variety of VoIP components and networks?

The solution to this problem is affected by the following *forces:*

- General security mechanisms, such as firewalls and Intrusion Detection Systems (IDS), cannot detect or prevent all attacks. They are unable to stop/detect unknown attacks, internal attacks, and attacks that come in the body of the messages (at a higher level). We need to analyze how an attack happened so we can try to stop it in the future, but we first need to collect the attack information.
- A real-time application, like VoIP, requires an automated collection of forensic data in order to provide data reduction and correlation. Current techniques dealing with evidence collection in converged networks are based on post-mortem (dead forensic) analysis. A potential source of valuable evidence (instant evidence) may be lost when using these types of forensics approaches.
- Even though there are a number of best practices in forensic science, there are no universal processes used to collect or analyze digital information. We need some systematic structure.
- The amount of effort required to collect information from different data sources is considerable. In a VoIP environment we need automated methods to filter huge volumes of collected data and extract and identify data of particular interest.
- The large amount of redundancy in raw alerts makes it difficult to analyze the underlying attacks efficiently [Wan05]
- A forensic investigator needs forensic methods with shorter response times because the large volume of irrelevant information and increasingly complex attack strategies make manual analysis impossible in a timely manner [Wan05].

Solution

Collect details about the attacker's activities against VoIP components (e.g., gatekeeper) and the voice packets on the VoIP network and send them to a forensic server. A forensic server is a mechanism that combines, analyzes, and stores the collected evidence data in its database for real-time response.

A common way of collecting data is to use sensors with examination capabilities for evidence collection. In VoIP forensic investigations, these devices will be deployed in the converged environment, thus reducing human intervention. These hardware devices are attached in front of the target servers (e.g., gatekeeper) or sensitive VoIP components, in order to capture all voice packets entering or leaving the system. These sensors are also used by the Intrusion Detection System (IDS) to monitor the VoIP network. Examiners can also use packet sniffers and Network Forensic Analysis Tools (NFAT) to capture and decode VoIP network traffic.

When the IDS detects any attempt to illegally use the gatekeeper or a known attack against VoIP components, it gives alarms to the forensic server, which in turn makes the evidence collector start collecting forensic data.

The evidence collector then collects and combines the forensic information from several information sources in the network under investigation. It will also filter out certain types of evidence to reduce redundancy.

Structure

Figure 2 shows the UML class diagram of the evidence collector (based on [Ren05]). The **Evidence Collector** is attached to hosts or network components (e.g., **gatekeeper**) at the node where we need to collect evidence in a **VoIP network**. Forensic data is collected using **embedded sensors** attached to key VoIP components or **NFAT** tools. VoIP components that are monitored can provide forensics information once an attack occurs. The Evidence Collector should be designed to extract forensic data and securely transport it (i.e., hash and encrypt) to the **forensic server** using a VoIP secure channel [Fer07b]. The forensic server combines the logs collected from the target servers and the VoIP network and stores them in its database to allow queries via command user interfaces. The network forensics server also controls the Evidence Collectors.

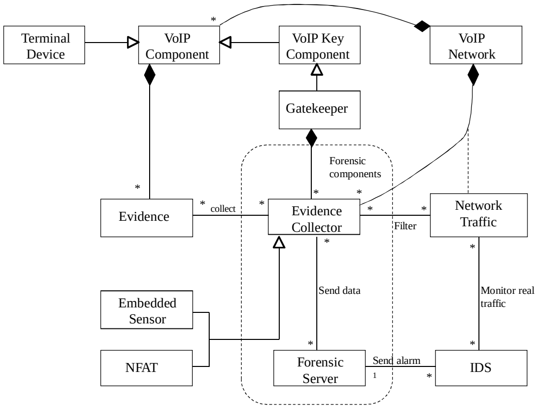


Figure 2 Evidence Collector Class Diagram

The **evidence** data collected from VoIP key components includes the IDS log files, system log files, and other forensic files. Other sensitive files may include the system configuration files and temp files. When attached to a terminal device, the Evidence Collector captures the **network traffic** to record the whole procedure of the intrusion and can be used to reconstruct the intrusion behavior [Ren05]. The evidence collector is also able to filter out certain types of evidence to reduce redundancy.

Implementation

After collecting the desired forensic data, the evidence collectors will send two types of data to the network forensics server, depending on the function performed. If the sensor is attached to a key VoIP component, it will collect logging system and audit data; otherwise (i.e., attached to a terminal device) it will act as packet sniffers do (with the Network Interface Card (NIC) set to promiscuous mode) or NFAT tools extracting raw network traffic data (e.g., entire frames, including the payloads, are captured with tcpdump). These data are used to discover and reconstruct attacking behaviors.

As mentioned before, after each attack against the VoIP network, the forensic data collected from key components and attacking sources may include logging data. The following data may also be useful to discriminate calls and call types:

- Terminal device information
  - Numbers called
  - Source and destination IP addresses
  - IP geographical localization
  - Incoming calls
  - Start/end times and duration
  - Voice mail access numbers
  - Call forwarding numbers
  - Incoming/outgoing messages
  - Access codes for voice mail systems
  - Contact lists

- VoIP data
  - Protocol type
  - Configuration data
  - Raw packets
  - Inter-arrival times
  - Variance of inter-arrival times
  - Payload size
  - Port numbers
  - Codecs

In order to maintain efficiency when capturing network traffic, we select the data to save, such as source and destination addresses and ports, and protocol type. The evidence collector can then extract all or selective voice packets (i.e., incoming or outgoing) over the VoIP network by applying a filter. The database on the forensics server will store the data sent by evidence collectors in order to perform the corresponding forensics analysis. We can use network segmentation techniques [Fer07b] to monitor the voice VLAN traffic independently from data VLAN traffic although the two share the same converged network.

Dynamics

The sequence diagram of Figure 3 shows the sequence of steps necessary to perform evidence collection in VoIP. In this scenario, as soon as an attack is detected against the gatekeeper by the IDS, the evidence collector starts capturing all activities of the possible attackers. The evidence collector will then send the collected data to the forensic server using a secure VoIP channel. Additionally, the collected forensic data is filtered and stored in the system database.

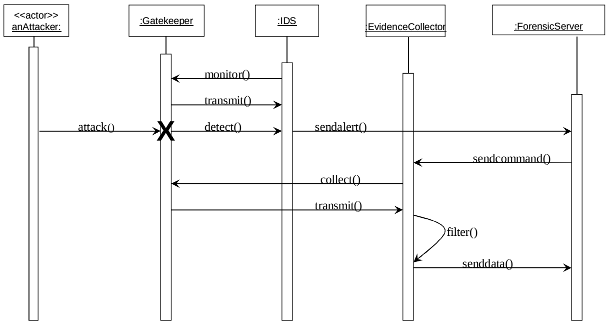


Figure 3 Sequence diagram for evidence collection in VoIP

Consequences

The *advantages* of this pattern include:

- The use of automated forensic tools as prescribed by this pattern allows effective real-time collection of forensic information which will reduce the investigation time in VoIP incidents.
- Significant logging information can be collected using this approach.
- The approach should be helpful to network investigators in identifying and understanding the mechanisms needed to collect real-time evidence in converged systems, because it provides a systematic way to collect the required information.
- The VoIP Evidence Collector pattern will also enable the rapid development and documentation of methods for preventing future attacks against VoIP networks.
- It is possible to investigate alleged voice calls using the evidence collector since voice travels in packets over the data network.
- For efficiency, the evidence collector can be set up for capturing selectively network packet streams over particular servers such as call, database, and web servers. The network forensics server can control the filter rules on the collector.
- On the other hand, based on the source/destination information, the evidence collector can filter the packets of a particular phone conversation.
- When encryption is present, the evidence collector can capture the headers and contents of packets separately.

The *disadvantages* of this approach are the limited scalability and relative inefficiency of the traffic's monitoring and recording. In large-volume traffic environments, there is a tradeoff between the monitored traffic and the available disk space [Ren05].

Known uses

The Solera Networks DS series [Sol09] is a commercial product line of network forensics appliances that capture, filter and store data in near real-time.

Related patterns

The VoIP Evidence Collector pattern has direct relationships to the VoIP Evidence Analyzer pattern, which will be presented next, and to the Secure VoIP Call pattern. Attack patterns could be used to select where to collect evidence.

IV. VoIP Evidence Analyzer

VoIP Evidence Analyzer pattern defines a structure and process to analyze the collected forensic data packets. It also presents a method of investigating an alleged IP attack scene and tracing back attackers.

Context

We are considering a VoIP environment in which the monitored network should not be aware of the collection process. We assume the existence of a mechanism to collect real-time evidence in converged systems and the preservation of such evidence in a secure way. We also assume a high-speed network with an authentication mechanism and secure transport channel among forensic components. We also assume that evidence has been collected by a VoIP Evidence Collector.

Problem

How to analyze evidence identified and extracted by the VoIP Evidence Collector in order to discover the attack source and other characteristics of the attack?

The solution is affected by the following *forces:*

- Two of the most costly, time-consuming and human-intensive tasks are the analysis and reconstruction of attacks in a compromised system.

- In order to correlate and interpret attacks against real-time converged networks, examiners need a structure for forensic analysis.
- An automated technique is fundamental to locate the attackers and reconstruct their criminal actions.
- We need shorter response times, a large volume of irrelevant information and increasingly complex attack strategies make manual analysis impossible in a timely manner [Wan05].
- Because the amount of data generated by VoIP networks is huge, storing network data for forensic analysis may be complicated.
- Encrypted packets are difficult to analyze.
- The forensic analysis process must guarantee data preservation and integrity.
- Attacks in converged networks are becoming more frequent and more complex to counter.
- A method is required for reusing network forensic knowledge and documenting forensic investigations.
- Forensic incidents in VoIP are often faced by examiners who do not have experience executing investigations or using similar forensic tools.

Solution

Combine (i.e., pre-process and store) all forensic logs and network traffic captured by the Evidence Collector into a forensic data repository (database and files) and analyze them using techniques such as log correlation and normalization [For04]. Logs are processed and converted into a simple format and then compared with the set of predefined attack patterns to identify possible security violations [Ren05]. The raw traffic data must also be converted into a readable format and stored in a separate database.

The evidence analyzer then performs automated inference based on the evidence database and presents results to the forensic investigator. The analysis process involves using automated methods to sift through large amounts of acquired data and extract and identify data of particular interest [Gra05].

Structure

Figure 4 shows a class diagram describing how an IP telephony and a forensic system integrate. This model shows the three primary forensic components: the **evidence collector**, the **forensic server** and the **network investigator**. The Evidence Collector is attached to a host that may be attacked in a VoIP network (e.g., **Gatekeeper**).

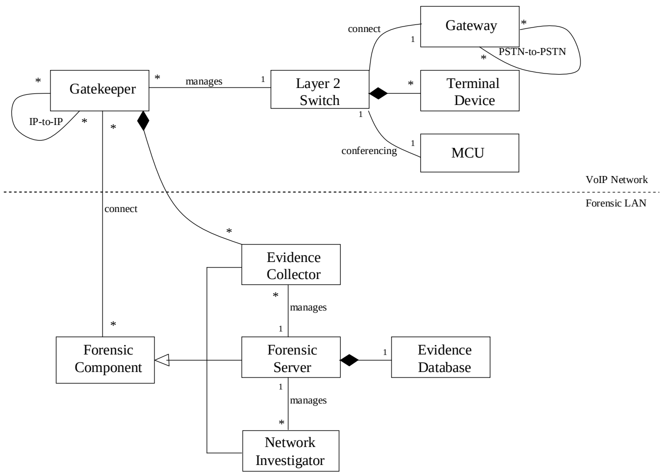


Figure 4 Class diagram for a VoIP network forensics system

The main function of the forensic server is combining the logging information collected from the VoIP network and its key components, and storing it in the evidence database. On the other hand, the network investigator acquires information about attackers and their sources by using techniques such as IP traceback and packet marking and by mapping topology to geographic locations so as to conduct further investigations.

Implementation

After the IDS gives the alert, the network forensics server sends a command to the network investigator (the response is in real-time). The network investigator receives information from the forensic server about sensitive spots on the VoIP network. Then the network investigator surveys the network in order to obtain useful information, such as the attacker location and phone numbers. The network investigator will also scan the network for mapping topology to find, for example, a false proxy server, or traceback the location of the attacker [Ren05]. Finally, the network investigator sends the scan and survey result to the forensic server using a VoIP secure channel [Fer07b]. This result will include such information as the topology of the network, the IP address, the MAC address, the possible geographic location of the IP.

The network forensics server can also analyze the attack behavior by replaying the attacking procedures. Network forensics tools can reorganize the packets into individual transport-layer connections between machines [Ren05]. With the appropriate tools, investigators can capture the packets and decode their voice packet payloads in order to analyze VoIP calls.

The forensics server provides correlations of forensics data in order to discover the attack behavior. This process will provide network investigators a better way to monitor voice traffic data and correlate events from VoIP security mechanisms (e.g., IDS).

To construct the given same events, it is necessary to correlate the different format logs to a single-layer data format by time, IP, and User ID. This task is known as normalization [For04]. Correlation in forensics is based on the knowledge of previous attacks gained by historical methods, geographical location, strength of signal, and the behavior of the attacker. Likewise, Attack Patterns [Fer07a] will provide prior knowledge of known exploits. VoIP Correlation Rules correlate events taken from multiple VoIP source devices, including Call Managers, IP PBXs, and voice gateways [Hic07]. These correlation rules will detect, for example, theft of service attempts as well as DoS attacks against VoIP servers.

Dynamics

The sequence diagram of Figure 5 shows the sequence of steps necessary to perform evidence analysis in VoIP. In the initial phase, the forensic evidence sent by the evidence collector is preprocessed and stored in the forensic server database. After scanning and surveying the network, the network investigator sends the results to the forensic server for further analysis and replay of the attacking procedures.

Consequences

The advantages of this pattern include:

- Investigators will be able to perform network forensic investigations (in real-time) in converged networks in a structured way.
- Designers will be able to correct weak points in a VoIP network perimeter in order to prevent future similar attacks.
- Automated evidence analysis will produce an immediate impact on the forensic investigator's ability to reduce response times [Wan05].
- The information that is collected can be used to anticipate adversarial actions, understand the current state of affairs, and help in determining appropriate courses of action [Gio02].
- The Evidence Analyzer can provide information about logs and for tracing back attackers.
- All the data from the monitored host, NFAT, and the network investigator will be stored as the evidence and analyzed for the final presentation.
- Encrypted data can be examined using traffic analysis. By examining the flow of packets over time, it is possible to determine such matters as when a user is using the VoIP device, whom the user communicates with, and the call history.

Possible disadvantages include:

- Disk storage space time overhead requirements may be a concern in some environments.
- Attack patterns need to be continually updated, and this will normally require human expertise.

Known uses

QRadar is a commercial product designed by Q1 labs to offer security monitoring for Voice over IP (VoIP) networks. This module combines network behavior analysis and security event correlation for monitoring across the network protocol, application, and security services layers of a VoIP network [Hic07].

Related patterns

The VoIP Evidence Analyzer pattern has direct relationships to the VoIP Evidence Collector pattern that was previously introduced and the Secure VoIP Call pattern. As indicated, attack patterns could help in forensic evidence analysis.

V RELATED WORK

The patterns have been inspired by ideas of Ren and Jin [Ren05], who developed a model based on distributed adaptive network forensics and active real time network investigation. Likewise, Tang [Tan05] developed a network forensics framework based on distributed techniques, which provides an integrated platform for automatic forensic evidence collection and data storage, supporting the integration of known attribution methods, and an attack attribution graph generation mechanism to illustrate hacking procedures. Finally, Wang and Daniels [Wan05] propose an evidence graph model to facilitate the presentation and manipulation of intrusion evidence. For automated evidence analysis, they developed a hierarchical reasoning framework that included local reasoning and global reasoning.

Kahvedzic and Kechadi prented a framework using ontologies for modeling , analyzing, and reusing forensic knowledge [Kah09]. However, their objective is to systematize and clarify the vocabulary used in describing forensic investigations.

Dlamini , Olivier, and Sibiya applied design patterns to add flexibility and reusability to traffic isolation so that forensic analysis can be performed more conveniently [Dla09}. We emphasize the collection and analysis of forensic information in a systematic way.

VI CONCLUSION AND FUTURE WORK

We have introduced the concept of forensic patterns as they relate to VoIP investigations. We illustrated these ideas using UML object oriented models. Likewise, some issues involved in VoIP forensic investigations were studied. Since attacks cannot be completely avoided, it is necessary to have appropriate forensics systems. By using these forensic patterns, investigators will have a structured method to collect, search and analyze network forensic data.

The proposed VoIP Evidence Collector pattern could use NFATs in combination with hardware sensors for real-time collection. Likewise, the VoIP Evidence Analyzer pattern analyzes the collected forensic data packets, and presents a process of investigating attacks against the VoIP network.

The usefulness of VoIP forensic patterns will depend on the creation and implementation of a VoIP pattern system [Pel09b]. These are the first steps toward a methodology for modeling network forensics. Future work will include the development of more general forensic patterns (i.e., not just for VoIP), as well as the corresponding wireless forensic patterns for a Tactical Internet environment (i.e., the integration of tactical digital radios and commercial Internet technology). In addition, we will develop a UML network forensic model based on this pattern system as a reference architecture for forensics. Other possibilities include combining our patterns with the design patterns of [Dla09] to improve their implementation.

REFERENCES

[Bog07] A.C. Bogen D. A. Dampier, and J.C. Carver, "Support for computer forensics examination planning with domain modeling: A report of one experiment trial", *Procs. of the 40th Annual Hawaii Int. Conf. on System Sciences (HICSS* 2007).

[Dla09] I. Dlamini, M. Olivier, and S. Sibiya, "Pattern-based approach for logical traffic isolation forensic modeling", *Procs. of the Third Int. Workshop on Secure System Mehologies Using Patterns (SPattern 2009),* IEEE, Sept. 2009, 145-149.

[DFRWS01] Digital Forensics Research Workshop. "A Road Map for Digital Forensics Research 2001." *Digital Forensics Research Workshop 6 November* (2001): http://www.dfrws.org /2001/dfrws-rm-final.pdf *(last accessed 8 June 2010).*

[Fer07a] E. B. Fernandez, J. C. Pelaez, and M. M. Larrondo-Petrie. "Attack patterns: A new forensic and design tool." *Proceedings of the Third Annual IFIP WG 11.9 International*. Conference on Digital Forensics, Orlando, FL, Jan. 29-31, 2007.

[Fer07b] E.B. Fernandez, J.C. Pelaez, and M.M. Larrondo-Petrie, "Security patterns for voice over IP networks", *Proceedings. of the 2nd IEEE Int. Multiconference on Computing in the Global Information Technology* (ICCGI 2007), March 4-9, Guadeloupe, French Caribbean.

[For04] D. Valentino Forte, The Art of Log Correlation - Tools and Techniques for Correlating Events and Log Files, IR Italy Project, 2004.

[Gam94] E. Gamma, R. Helm, R. Johnson, and J. Vlissides. Design Patterns: Elements of Reusable Object-Oriented Software, Addison-Wesley, Boston, Mass., 1994.

[Gra05] T. Grance and S. Chevalier. "Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response." *Recommendations of the National Institute of Standards and Technology*. August, 2005.

[Hic07] A. Hickey. "VoIP security monitoring gets proactive." SearchVoIP.com, 25 Jan 2007 *(last accessed 8 June 2010). http://searchunifiedcommunications.techtarget.com/news/article/0,289142,sid186_gci1240544,00.html*

[Kah09] D. Kahvedzic and T. Kechadi, "DIALOG: A framework for modeling, analysis and reuse of digital forensic knowledge*", Procs. of the 2009 Digital Forensics Research Workshop (DFRWS'09) , (last accessed 8 June 2010)* http://www.dfrws.org/2009/proceedings/p23-kahvedzic.pdf

[Pel09a] J.C. Pelaez and E.B. Fernandez. "VoIP Network Forensic Patterns." *Proceedings of the Fourth International Multi-Conference on Computing in the Global Information Technology (ICCGI 2009).* Cannes, France, August 23-29, 2009.

[Pel09b] J.C. Pelaez, E.B. Fernandez, and M.M. Larrondo-Petrie, "Misuse patterns in VoIP", accepted for Wiley's Security and Communication Networks Journal.

[Ren05] W. Ren, H. Jin. "Distributed Agent-based Real Time Network Intrusion Forensics System Architecture Design." *Proceedings of the 19th International Conference on Advanced Information Networking and Applications* (AINA'05). March, 2005.

[Sch06] M. Schumacher, E.B. Fernandez, D. Hybertson, F. Buschmann, and P. Sommerlad, Security Patterns: Integrating Security and Systems Engineering, Wiley publishing, New York, 2006.

[Sol09] Solera Networks. "DS Series Network Forensics Appliances."http://www.soleranetworks.com/products/forensics-appliances.php *(last accessed 8 June 2010).*

[Tan05] Y. Tang and T. E. Daniels, "A Simple Framework for Distributed Forensics," icdcsw, vol. 2, pp.163-169, Second International Workshop on Security in Distributed Computing Systems (SDCS) (ICDCSW'05), 2005.

[Wan05] W. Wang and T. Daniels. "Building Evidence Graphs for Network Forensics Analysis." *Proceedings of the 21st Annual Computer Security Applications Conference* (ACSAC 2005). September 2005.