Fourth LACCEI International Latin American and Caribbean Conference for Engineering and Technology (LACCET'2006)

"Breaking Frontiers and Barriers in Engineering: Education, Research and Practice"

21-23 June 2006. Mayagüez, Puerto Rico.

Wireless VoIP Network Forensics

Juan C Pelaez, M.C.S.
Florida Atlantic University, 777 Glades Road SE-300, Boca Raton, FL 33431-0991 USA
jpelaez@arl.army.mil,

Eduardo B. Fernandez, PhD
Florida Atlantic University, 777 Glades Road SE-408, Boca Raton, FL 33431-0991 USA
ed@cse.fau.edu

Abstract

Voice over Internet Protocol over Wireless (VoIPoW) networks is becoming the most popular system for mobile communication in the world. However, investigations into attacks on wireless VoIP networks are still in their infancy. Wireless devices are commonly use by delinquents, and it is therefore necessary for network investigators to understand which evidence can be obtained from the VoIP system. This survey paper discusses network security investigations in a wireless converged environment.

Keywords

IP Protocol, networks, object-oriented patterns, security, VoIP.

1. Introduction

Flexibility is a necessary element in today's mobile communications world. Voice over Internet Protocol (VoIP) has had a strong effect on wireless communications by allowing human voice and video to travel over existing packet data networks along with traditional data packets. VoIP over wireless (VoIPoW) networks is becoming the most popular system for mobile communication in the world. However, studies of attacks on wireless VoIP networks are still in their infancy. Wireless devices are commonly used by delinquents, and it is therefore necessary for network investigators to understand which evidence can be obtained from the VoIP system after an attack has occurred.

The increase in cellular and wireless hand-held devices provides a unique challenge for network investigators. Among the several issues that need to be addressed when deploying this technology, security is one of the most critical. While an attack on a wired network is investigated by tracing it back to a physical location, no physical access is required when a wireless medium is attacked. It is then harder to extract evidence in this case.

Network forensics support VoIP investigations by providing information about the location and the way that attackers perform their crimes. Network forensic models allow not only the detection of complex attacks, but the understanding of what happened after a system is breached. The collection of this evidence is crucial in the prosecution of criminals. Thus, network forensics not only helps to find criminal but also to stop network crimes and reduce their rates.

We explore here network forensics in VoIPoW with the technology that already exists, and identify some of the issues that will have to be resolved in the future. To effectively analyze the network investigations in VoIPoW, we start by giving an overview of VoIP. We then analyze VoIPoW and some of the most popular forms of implementing this technology. Further, we explore the type of evidence that can be obtained in the network, in the Subscriber Identity Module (SIM) card, and in the wireless device. Finally, we introduce some network forensics models based on distributed adaptive network forensics and active real time network investigation. We end with some conclusions.

2. VoIP overview

VoIP is defined as the transport of voice over IP-based networks. Any data network that uses IP can be used to establish this service. VoIP can be achieved on any data network that uses IP, such as the Internet, intranets and Local Area Networks (LAN), where digitized voice packets are transmitted. VoIP can be considered as one more transport technique within the IP layer.

In carrier networks, VoIP has been mainly deployed in enterprise networks or as a trunking technology to reduce transport costs in voice backbone networks [Dre03]. Also, the hardware for a VoIP system is less expensive that of a GSM or cellular service.

Existing network infrastructures can be used to carry data, voice and video traffic, which are very important for users. Savings come from eliminating the need to purchase new Private Branch Exchanges (PBX) equipment, and from reducing staff and maintenance costs, as only one network needs to be supported [Wei01].

2.1 VoIP Protocols

VoIP uses the Real-Time Protocol (RTP) for transport, the Real-Time Transport Protocol (RTCP) for Quality of Service (QoS) and H.323, SIP, MGCP (Media Gateway Control Protocol/Megaco) for signaling. These protocols operate in the application layer; that is, on top of the IP protocol.

A class diagram for VoIP components in an H.323 is shown in Figure 1. The layer 2 QoS enabled switch provides connectivity and network availability between H.323 components. The IP-PBX server acts like a call processing manager providing call setup and routing the calls throughout the network to other voice devices.

Although most VoIP implementations today use the H.323 protocol for IP services, SIP is more appropriate for wireless applications due partly to its flexibility and lower implementation costs.

2.2 Wireless VoIP

VoIP has not only been gaining ground on landline networks but also is getting high interest for wireless networks. In addition to the advantages of VoIP, VoIPoW provides service flexibility.

With this technology, users will be able to use a diversity of wireless devices including cellular phones, two-way radios, PDAs, laptop computers, and similar. The low cost of transport and switching is another benefit of this technology.

There exist many different forms of implementing VoIP in wireless communications and networking. Two popular forms of wireless VoIP are described below.

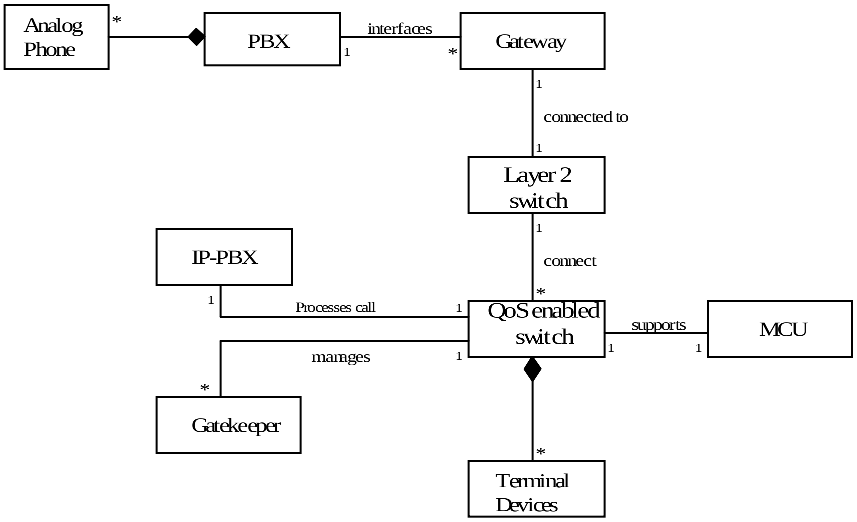

Figure 1 Class Diagram for a H.323 architecture

2.2.1 VoIP in WLANs

VoIPoW using the 802.11 standard for wireless local area networks (WLANs) is an important technology used for converged voice and data on mobile computers. Using the installed 802.11 wireless infrastructure for both voice and data is an ideal approach to solving most communication requirements for mobile users; but this also increases many existing VoIP security concerns.

Figure 2 shows a class diagram for a VoIPoW application using the WLAN approach. Packet networks are used to transmit the compressed voice packets. The fixed IP terminals (i.e. hardphones and softphones) exchange voice samples with wireless IP terminals using the RTP protocol.

2.2.2 VoIP in Cellular Networks

In the Global System for Mobile communication (GSM) approach, packet networks are used to transmit the compressed voice packets offering bandwidth savings. The base station controller (BSC) or base transceiver station (BTS) provides wireless access to the IP network. Connectivity between the Base Stations (BTSs), Base Station Controllers (BSCs), and the Mobile Switching Center (MSC) is also achieved using IP networks. The fixed IP terminals (i.e. IP phones/ Softphones) exchange voice samples with cellular IP terminals using RTP. A class diagram (adapted from a figure in [Pel04]) for the GSM approach is shown in Figure 3.

GSM provides mobility to users allowing them to use either GSM devices or H.323 terminals (IP phones or PCs) to access telecommunication services, using VoIP. Thus, a user can move from a GSM network into an IP network and can use his H.323 terminal to receive calls and other VoIP services.

At the present time, some wireless communication companies are offering "dual-mode" wireless phone solutions for enabling seamless roaming between wide-area cellular networks and Wi-Fi networks (e.g. DSL). These mobile devices are capable of automatically detecting Wi-Fi access points in order to connect to the IP network.

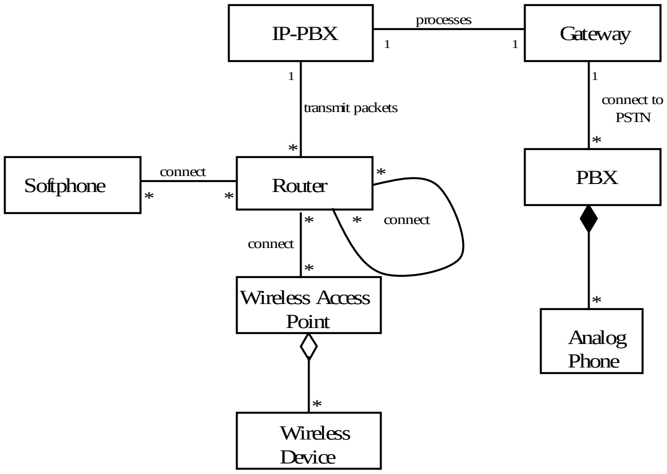

Figure 2 Class diagram for a VoIPoW application using WLANs.

The main functions in a cellular network that enable mobility are the home location register (HLR) and the visitor location register (VLR). Through an overlay of these functions on the landline network, in the form of a third-generation partnership project (3GPP)-compliant IMS network environment, operators are able to offer subscribers possessing a Wi-Fi-enable cell phone access to less expensive fixed-line services from virtually any location served by a broadband wireless network [Ver05].

The security element of this service is a routing directory which keeps the subscriber-registry functions that perform device authentication and periodically update the current location of the mobile phone within the IP and GSM networks. Figure 4 shows a class diagram for the Verisign Network Routing Directory [Ver05] which supports VoIP (SIP and electronic numbering) as well as cellular-based (ANSI-41 and GSM-MAP) location-discovery services, providing authentication and routing information that may be used to establish connectivity across various wireline and wireless network technologies.

3. VoIP Security

As VoIP in a wireless environment operates on a converged (voice, data, and video) network, voice and video packets are subject to the same threats than those associated with data networks. In this type of environment not only is it difficult to block network attackers but also in many cases, examiners are unable to find them out. Likewise, all the vulnerabilities that exist in a VoIP wired network apply to VoIPoW technologies plus the new risks introduced by weaknesses in wireless protocols.

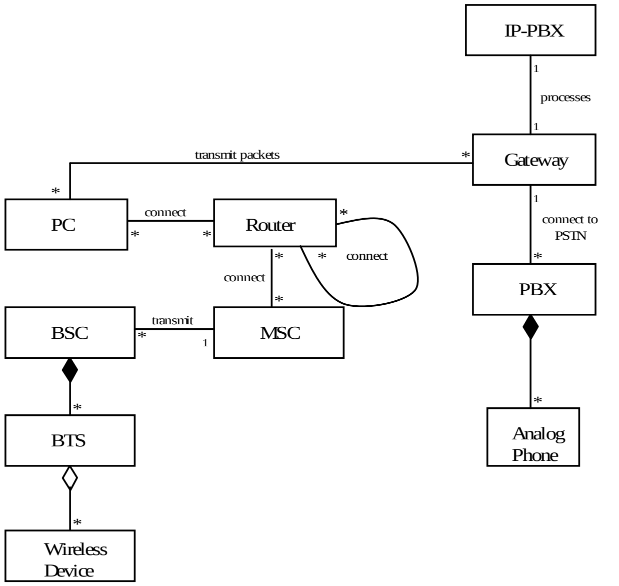

Figure 3. Class diagram for a VoIPoW application using GSM.

Thus, VoIPoW networks need to be protected against confidentiality, authentication, integrity and repudiation attacks. One way to achieve this is by using security mechanisms such as authentication, tunneling and segmentation [Pel05]. Network forensics add another dimension.

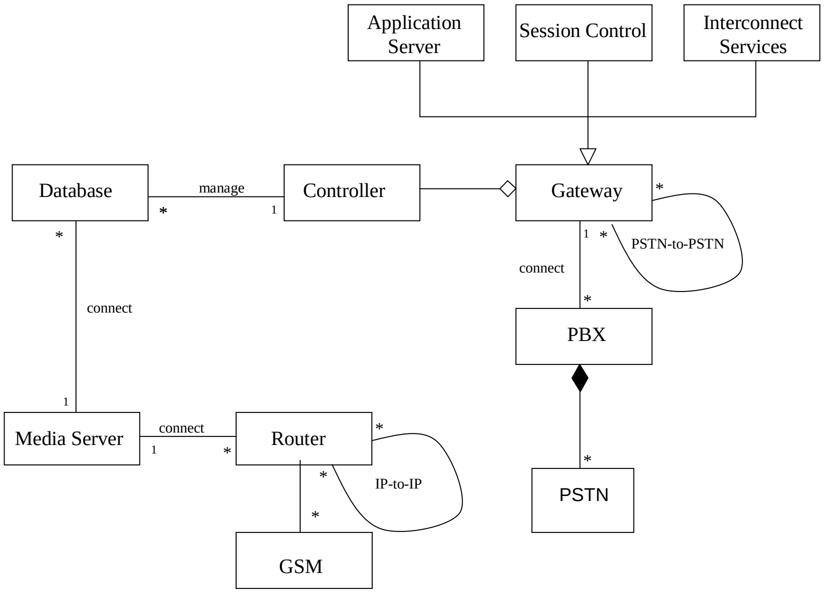

Figure 4 Class Diagram for the Verisign Network Routing Directory

3.1 Network forensics

Network forensics is the act of capturing, recording, and analyzing information collected on active networks from various intrusion detection, auditing, and monitoring points in order to discover the source of security breaches or other information assurance problems [Ran06]. Network forensics technology is applicable not only to law enforcement, but also to industry, the military, and to some degree private users. Examples of these network analysis procedures are: the examination of router logs, firewall logs, or eavesdropped data from a network.

Network forensics support VoIP investigations by providing information about the location and the way that attackers perform their crimes. The collection of this evidence is crucial in the prosecution of criminals. Thus, network forensics not only helps to find criminals but also to indirectly stop network crimes and reduce their rates.

Network forensics can illuminate issues such as bandwidth use in terms of machines, protocols, users, or content. It can summarize findings that might be of concern, such as unauthorized services, cleartext-password protocols, or implementations that violate protocol standards [Cor02].

The collection of data in real time and the use of automatic mechanisms are vital when conducting network forensics investigations in a VoIP environment. This will result in a better and faster response to network attacks.

Major objectives of network forensics analysis can be summarized into two fundamental problems: attack group identification and attack scenario reconstruction. Attack scenario reconstruction is the process of inferring step-wise actions taken by the attacker to achieve his malicious objective. Attack group identification is the task of discovering the group of hosts involved in the attack and determining the roles of each host in the group [Wan05].

3.2 Network Analysis Tools

After a VoIP system has been attacked, the first step to obtain forensic evidence is to listen on the network interface and capture relevant traffic data using predefined traffic patterns. Network investigators usually have a number of sources of information on network traffic that may be useful. Due to the fact that voice travels in packets over the data network, data examiners can use network forensics and other packet-sniffing tools to identify, store and playback voice communications traversing the network. With the appropriate tools, investigators could capture the packets and decode their voice packet payloads in order to analyze VoIP calls.

Packet Sniffers are also referred to as network monitors or packet analyzers. They are software applications that capture and decode network traffic. Packet sniffers use a network adapter card in promiscuous mode to capture voice packets traveling the IP network. Packet sniffers are good tools for network investigators who want to monitor the information that enters and leaves the system.

Network Forensic Analysis Tools (NFAT) typically provide the same functionality as packet sniffers and protocol analyzers. NFAT software is primarily focused on collecting and analyzing network traffic [Nis05].

NFAT must perform three tasks well. It must capture network traffic; it must analyze the traffic according to the user's needs; and it must let system users discover useful and interesting things about the analyzed traffic [Cor02].

One of the currently most popular packet-collection tools is tcpdump, this software can be downloaded freely on the Internet and is available on most Unix and Windows platforms.

With tcpdump, examiners can identify the IP and MAC address of the participant phones. For example, the tool "voice over misconfigured Internet telephones" (a.k.a. “vomit”), takes an IP phone conversation trace captured by the tool tcpdump, and reassembles it into a wave file which makes listening easy [Pog03]. Figure 5 shows the sequence (refer to the H.323 architecture in class diagram 1) of steps necessary to monitor a VoIP conversation.

In practice, this reconstructive traffic analysis is often limited to data collection and packet level inspection; however, a NFAT can provide a richer view of the data collected, allowing you to inspect the traffic from further up the protocol stack [Cor02].

3.3 Other network forensic methods

3.3.1 IP Traceback and Packet Marking

IP traceback and packet marking are important network forensic analysis techniques used for attack attribution. IP trace back is a method in which network investigators trace a flow of anonymous voice packets back to their origin. IP trace back can be grouped into two main categories. One in which no extra network packets are generated and the other in which a few extra network packets are generated. The former is either based on probabilistic packet marking which overloads existing header fields (e.g. IP fragment ID field) to succinctly encode the path traversed by a packet in a manner that will have minimal impact on existing users or based on keeping the digest of all the IP packets in the infrastructure itself (e.g. routers). Thus, given an input IP packet, it can be reliably traced back to its origin. In the latter technique, a router picks a network packet with a small probability (e.g. 1 in 20,000) and sends a traceback packet as an ICMP message to the destination of the packet with the router’s own IP as the source. During a denial of service attack the victim will receive sufficient traceback packets to reconstruct the attack path [Sha03].

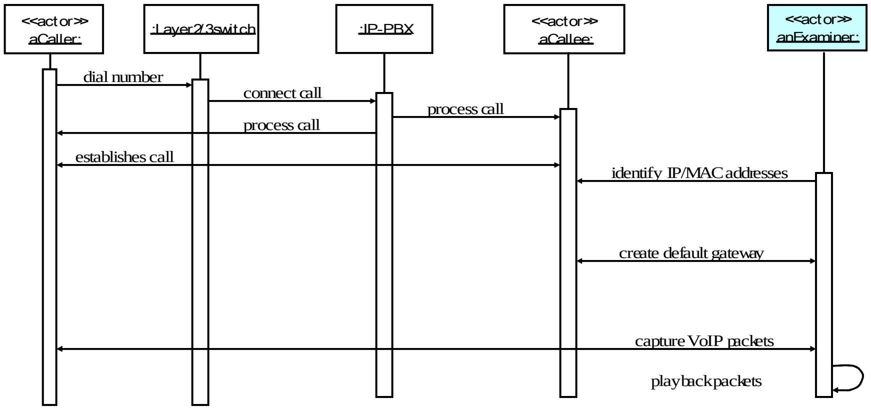

Figure 5 Sequence diagram for call monitoring

Alex C. Snoeren [Sno02] developed what he called a “Source Path Isolation Engine (SPIE)” to perform IP traceback using a Bloom Filter as the data storage mechanism.

In summary, locating attackers with the IP trace back technology is a potential security mechanism to counter DoS and many other type of attacks. IP trace back works even when criminals conceal their geographic locations by spoofing source addresses.

3.3.2 Intrusion Detection Systems

IDS is another important evidence tools for network forensics analysis. IDS is a method that inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network attack.

IDSs are classified into two categories: anomaly detection and misuse (knowledge-based) detection. Anomaly detection systems requires the building of profiles for each user group on the system. This profile defines an established baseline for the activities that a normal user routinely does to perform his job [Cor02]. But these systems have several drawbacks: These IDS alerts are not well adapted for forensics investigation, they are complicated, impractical and have a high false negative rate.

In contrast, misuse detection methods, also known as signature-based detection, look for intrusive activity that matches specific signatures. These signatures are based on a set of rules that match typical patterns and exploits used by attackers to gain access to a network [Fer05]. The disadvantage with misuse detection is that they cannot detect new attacks because they don't have a known signature.

The best solution is to combine signature based systems and anomaly detection systems that can decrease false alarm rates using a lightweight IDS, e.g. snort [Cas06]. Snort can be used as a straight packet sniffer, a packet logger and a full-blown network intrusion detection system.

The problem is that snort is still a misuse detection system and it only catches known attacks or unusual behavior. In general, with IDSs there exist much redundancy and high false alarm rates while relevant information may be missing or incomplete.

3.4 Government Surveillance

Government Surveillance is a special case of network forensics. Communications Assistance for Law Enforcement Act (CALEA) is another term for this electronic surveillance. It means that the legal enforcement agent taps into a communication channel to intercept, but not alter, the information [Sco04].

The wiretap facility is based on the MAC address of the cable modem so it can be used for either data or digitized voice connections. This feature is controlled by the interface command, cable intercept, which requires a MAC address, an IP address, and a UDP port number as its parameters. When activated, the router examines each packet for the desired MAC address; when a matching MAC address is found (for either the origination or destination endpoint), a copy of the packet is encapsulated into a UDP packet which is then sent to the server at the specified IP address and port [Cis04].

Figure 6 shows how the CALEA model components (i.e. Delivery Function, Collection Function and Law Enforcement Agency) integrate with a VoIP system providing a transparent lawful interception. Calls are routed via an access gateway that hides any intercepts in place.

Wiretaps are divided in two categories:

Call detail is a tap in which the details of the calls made and received by a subscriber are passed to LEA (Referred to as pen register and trap and trace in the U.S.). In the second kind of tap Call content, the actual contents of a call are passed to LEA. The suspect must not detect the tap, so the tap must occur within the network and not at the subscriber gateway. Also, the tap may not be detectable by any change in timing, feature availability or operation.

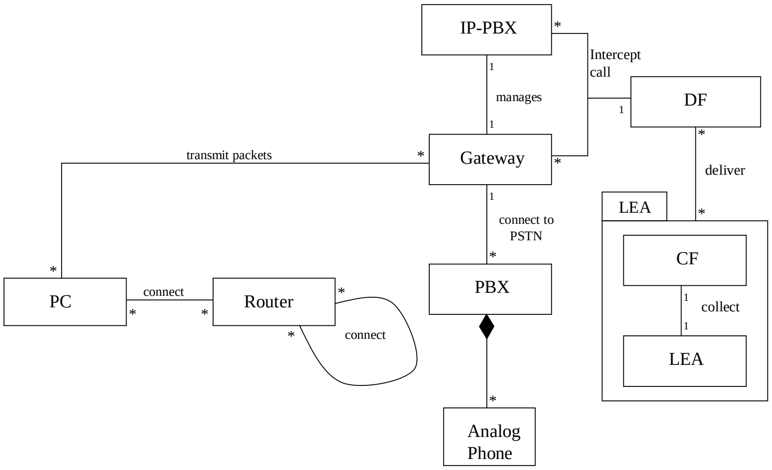

Figure 6 Class Diagram for CALEA Model

In order for LEA to tap the content of calls without the subscriber noticing any change, all calls must be routed via a device competent in duplicating the content and passing it to that agency.

Lawful interception requirements in many countries could prevent a public carrier from allowing direct connection between IP phones [Dre03]. With regard to fighting terrorism, support for CALEA over IP is a matter of special concern because many terrorist activities have taken place by using the Internet. Thus, lawful interception in VoIP is vital for national security but because it threatens user's privacy it must be performed only in authorized cases.

4. Network Forensic Models

In today's mobile communications world network investigators are in need for network models that allow not only the detection of complex attacks, but also that support forensic evidence collection, storage and analysis. The analysis of different types of records in mobile devices and the use of these records to reconstruct any attack related event are forensic operations often executed manually. Those forensic manual methods make the analysis almost impossible due to the large volume of data in IP networks.

Some papers have been written about network forensic models by different network security specialists and organizations, but in general, none of these authors did a systematic work of identifying formal security patterns for attacks against the VoIP network infrastructure. One of the earliest discussions about this topic is a paper by Stephenson [Ste03] discussing an approach to post-incident root cause analysis of digital incidents (a.k.a. digital post mortems) that has structure and rigor and the results of which can be modeled formally using Colored Petri Nets. He focuses upon the investigative approach in forensic digital analysis and the modeling of the outcome.

Tang and Daniels [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. Most recently, Ren and Jin [Ren05] developed a model based on distributed adaptive network forensics and active real time network investigation. However, none of these authors have discussed object-oriented models or attack patterns for VoIP systems. We will discuss the Ren-Jin model next.

4.1 Ren-Jin model

This model is designed to capture network traffic and log the corresponding data. There are four elements in this network forensics system:

Network forensics server, which integrates the forensics data and analyzes it. It also guides the network packet filter and captures the behavior on the network monitor. It can launch the investigation program on the network investigator as the response to the sensitive attacks.

Network forensics agents are responsible for the data collection, data extraction and data secure transportation. These agents are deployed on the monitored host and network.

Network monitor is a packet capture machine to adaptively capture the network traffic.

Network investigator is the network survey machine. It investigates a target when the server gives the command. It launches real time investigation responses to network intrusions.

Figure 7 shows a class diagram with the architecture of the network intrusion forensics system. There are two local area networks in the architecture. One LAN is the monitored honeynet network. The other is a forensics LAN, which is high-speed and utilizes SSL (Secure Socket Layer) techniques to secure transportation.

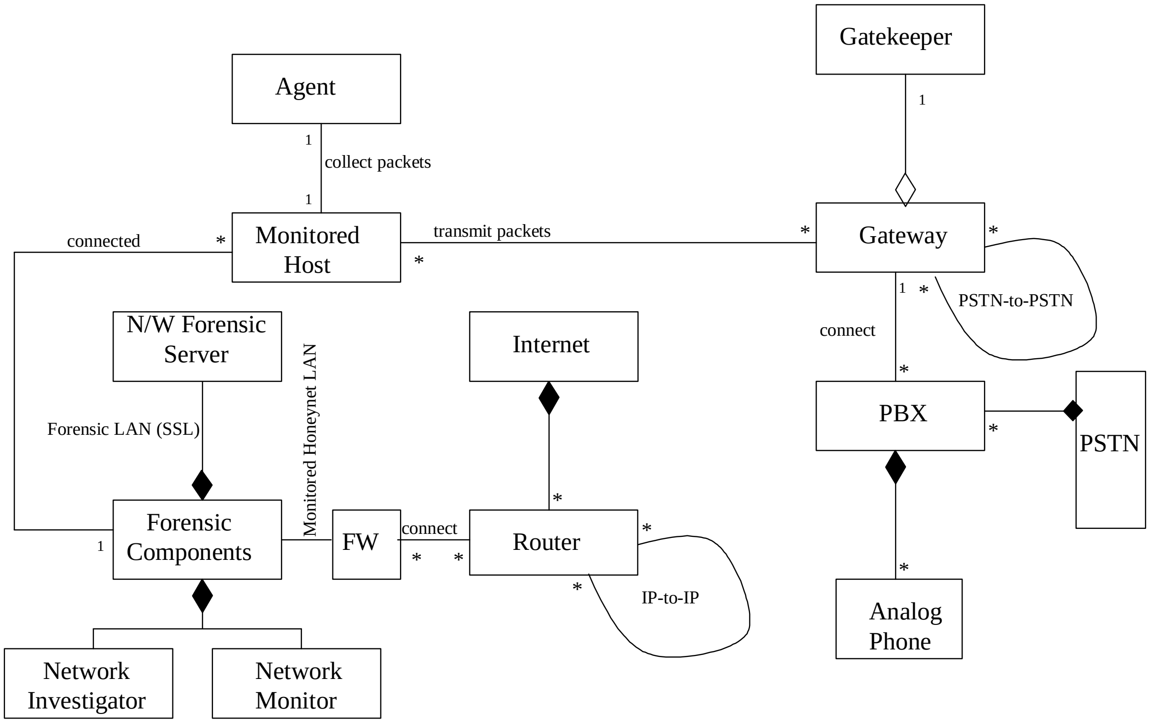

Figure 7 Ren-Jin forensic model

The network forensics and honeynet systems have the same features of collecting information about the system misuses. The honeynet system lures attackers and gains information about new types of intrusions. The network forensics system analyzes and reconstructs attack behaviors. The integration of these two systems helps to build an active self-learning and response system to profile the intrusion behavior features and investigate the attack original source.

6. Conclusions

In conclusion, due to the fact that VoIP will be the most popular system for mobile communication in the near future, it is necessary to study the mechanisms and tools for forensic analysis of converged networks.

Identifying the attacker is not an immediate primary concern after a VoIP system has been cracked. However, network investigators must use network forensic tools to establish the identity and location of the attacker in order to stop ongoing attacks.

Network forensic tools (e.g. NFAT software) and methods like IDS and IP trace back are valuable to network investigators in collecting network traffic data. This information found in VoIP systems has a great potential to be used as evidence.

UML models could increase the amount of evidence recovered without significantly increasing the combined effort of planning and executing a large-scale examination. The value of this additional effort may also be realized when forensic patterns are reused on similar cases.

This paper presents effective ways in which network investigators can more effectively implement the use of network forensics as a secure and convenient method of collecting digital evidence in a wireless VoIP environment.

References

[Cas06] Caswell Brian. “Snort Users Manual,

http://www.snort.org/docs/snort_manual/

[Cis04] Cisco Systems. “Configuring the Cisco uBR-MC28C Cable Modem Card,” May 2004.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121newft/121limit/121ec/121ec3/flmc28.pdf

[Cor02] Corey, Vicka. “Forensic Analysis.**”** Sandstorm Enterprises, December 2002
http://computer.org/internet/ NOVEMBER

[Dre03] Drew, Paul, “Next-Generation VoIP Network Architecture” March, 2003

http://www.msforum.org/

[Fer05] E.B.Fernandez and A.Kumar, “A security pattern for rule-based intrusion detection”, Procs. of the Nordic Pattern Languages of Programs Conference (VikingPLoP 2005)

[IEC00] IEC. “Global System for Mobile Communication (GSM)”, September 2000

http://www.iec.org/

[Nis05] National Institute of Standards and Technology, “Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response”, August 2005

http://csrc.nist.gov/publications/drafts.html

[Pel04] Pelaez, Juan. “Security in VoIP networks”. Master’s thesis, Florida Atlantic University, August 2004.

[Pel05] Pelaez, Juan and Fernandez, Eduardo. “Security in VoIP networks”. Proceedings of LACCEI International Latin American and Caribbean Conference for Engineering and Technology, June 2005

[Pog03] Pogar, Noel, "Data Security in a Converged Network" July 23, 2003

http://www.siemens.com/

[Ran06] Ranum, Marcus. "Network Flight Recorder."
http://www.ranum.com/

[Ren05] Ren, Wei. "Honeynet based Distributed Adaptive Network Forensics and Active Real Time Investigation." March 2005
http://delivery.acm.org/10.1145/1070000/1066749/p302ren.pdf?key1=1066749&key2=2811515411&coll=GUIDE&dl=GUIDE&CFID=69531752&CFTOKEN=57775863

[Sha03] Shanmugasundaram, Kulesh. "ForNet: A Distributed Forensics Network." Department of Computer and Information Science. Polytechnic University, Brooklyn, NY. 2003

[Sco04] Scoggins, Sophia. "Security Challenges for CALEA in Voice over Packet

Networks". April 16, 2004

[Ste03] Stephenson, Peter. "Modeling of Post-Incident Root Cause Analysis." October 2003

http://www.ijde.org

[Tan05] Tang, Yongping. "A Simple Framework for Distributed Forensics." January 2005

http://doi.ieeecomputersociety.org/10.1109/ICDCSW.2005.24

[Ver05] Verisign. "Wi-Fi VoIP and Cellular Network Integration: The Power of Dual-Mode

Handsets and Wi-Fi"

www.verisign.com/static/031270.pdf

[Wan05] Wang, wei. "Building Evidence Graphs for Network Forensic Analysis." May 2005

http://www.acsac.org/2005/abstracts/125.html

[Wei01] Weiss, Eric, "Security concerns with VoIP" August 20, 2001

http://www.sans.org/rr/papers/index.php?id=323

Biographic Information

Juan C PELAEZ. Mr. Pelaez is a PhD candidate in the Department of Computer Science and Engineering of Florida Atlantic University. He is a research scientist for the U.S. Army Research Laboratory. He is also part of the Secure Systems Research Group at Florida Atlantic University.

Eduardo B. FERNANDEZ (http://polaris.cse.fau.edu/~ed), is a professor in the Department of Computer Science and Engineering at Florida Atlantic University, and the leader of the Secure Systems Research Group (http://www.cse.fau.edu/~security). He has published numerous papers and four books on different aspects of security, object-oriented analysis and design, and fault-tolerant systems. He holds a Ph.D. degree from UCLA. His industrial experience includes 8 years with IBM and consulting with several companies.

Authorization and Disclaimer

The authors authorize LACCEI to publish the papers in the conference proceedings on CD and on the web. Neither LACCEI nor the editors will be responsible either for the content or for the implications of what is expressed in the paper.