15

Developing New Approaches for Intrusion Detection in Converged Networks

Juan C. Pelaez
U.S. Army Research Laboratory
APG, MD 21005,
USA

1. Introduction

An Intrusion Detection System (IDS) is an important evidence collection tool for network forensics analysis. An IDS operates by inspecting both inbound and outbound network activity and identifying suspicious patterns that may be indicative of a network attack.
For each suspicious event, IDS software typically records information similar to statistics logged by firewalls and routers (e.g., date and time, source and destination IP addresses, protocol, and basic protocol characteristics), as well as application-specific information (e.g., username, filename, command, and status code). IDS software also records information that indicates the possible intent of the activity [Gra05].
IDS data is often the starting point for examining suspicious activity. Not only do IDSs typically attempt to identify malicious network traffic at all transmission control protocol/Internet protocol (TCP/IP) layers, they also can log many data fields (including raw packets) that can be useful in validating events and correlating them with other data sources [Ken06].
IDSs are classified into two categories—anomaly detection and misuse (knowledge-based) detection. Anomaly detection systems require the building of profiles for the traffic that commonly traverses a given network. This profile defines an established baseline for the communication and data exchange that is normally seen over a period of time. These systems have several drawbacks: the IDS alerts are not well adapted for forensics investigation (i.e., sometimes vague), they are complicated (i.e., cannot be communicated easily to nontechnical people), 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 systems is that without a signature, a new attack method will not be detected until a signature can be generated and incorporated.
VoIP has had a strong effect on tactical networks by allowing human voice and video to travel over existing packet data networks with traditional data packets. Among the several issues that need to be addressed when deploying this technology, security is perhaps the most critical. General security mechanisms, such as firewalls and Intrusion Detection Systems (IDS), cannot detect or prevent all attacks. Current techniques to detect and counter

attacks against the converged infrastructure are not sufficient; in particular, they are deficient with respect to real-time network intrusion detection, especially where very high dimensional data are involved, because of computational costs. In addition, they are unable to stop/detect unknown, internal attacks, and attacks that come in the body of the messages (e.g., steganophony attacks [Pel09]). It is indispensable to analyze how an attack happened in order to counter it in the future.

In order to effectively counter attacks against the converged network, a systematic approach to network forensic collection and analysis of data is necessary. 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. In this chapter we will study how attacks against the converged network can be automatically detected in order to create a more secure VoIP system. Our primary focus is on attacks that target media and signaling protocol vulnerabilities.

To effectively study new approaches for intrusion detection in VoIP, this chapter starts by analyzing the attacks against the VoIP infrastructure from a hybrid architecture perspective, which will give a clear set of use cases to which we can relate these attacks. Then, network forensic challenges on converged networks are analyzed based on the Digital Forensics Research Workshop framework and on the forensic patterns approach. Further, an analysis of the protocol-based intrusion detection method is presented. Then, statistical methods for intrusion detection, such as stream entropy estimation and dimensionality reduction, are discussed. Finally, the converged experimentation testbed used for prototype tools and commercial software testing is introduced. This chapter ends with some conclusions and ideas for future work.

2. Attacks against the VoIP network

As VoIP 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 [Fer07]. 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 1 shows a Use Case diagram for a simplified VoIP system with typical use cases and internal and external roles. For example, the subscriber role can be classified as internal or remote, and also according to the type of device used. In addition to these roles, the use case diagram can be used to systematically analyze the different types of attacks against the VoIP network, following the approach in [Fer06].

Based on the Use Case Diagram of Figure 1, we can identify potential internal and external attackers (hackers). Internal attackers could be a subscriber with a malicious behavior. Therefore, this Use Case Diagram will help us to determine the possible attacks against the VoIP infrastructure.

Most of the possible attacks against the VoIP infrastructure will be listed systematically. Although completeness cannot be assured, we are confident that at least all important possible attacks were considered. This research does not guarantee to provide a complete list of every possible threat in VoIP. The threats that we assume are based on the knowledge of the VoIP application, and from the study of similar systems.

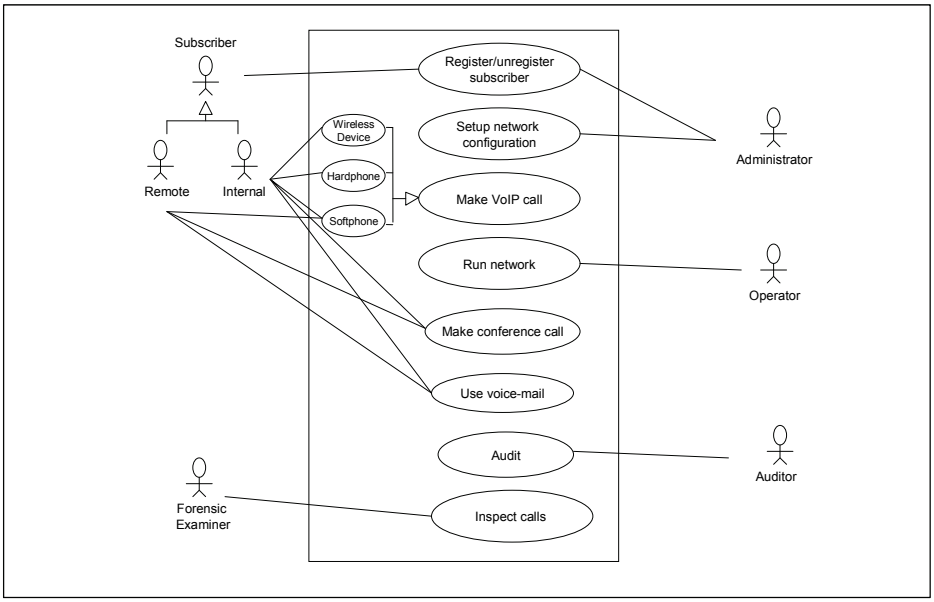


Fig. 1. Use case diagram for a VoIP system

It should be noted that only attacks against the VoIP system are considered. Attacks to systems that collaborate with this system are beyond our control (e.g. attacks against radio networks). Additional security issues relevant to telecom, physical networks, and switches are beyond the scope of this dissertation.

Based on the Use Case Diagram of Figure 1, we can determine the possible attacks against the VoIP infrastructure and classified as: Registration Attacks, Attacks when Making/Receiving a voice call and attacks against Audit.

2.1 Attacks when making/receiving a VoIP Call

Many of the already well-known security vulnerabilities in data networks can have an adverse impact on voice communications and need to be protected against [Pog03]. The attacks when making/receiving a voice call can be classified as follows:

Theft of service is the ability of a malicious user to place fraudulent calls. In this case the attacker simply wants to use a service without paying for it, so this attack is against the service provider.

Masquerading, occurs when a hacker is able to trick a remote user into believing he is talking to his intended recipient when in fact he is really talking to the hacker. Such an attack typically occurs with the hacker assuming the identity of someone who is not well-known to the target. A masquerade attack usually includes one of the other forms of active attacks [Sta02].

IP Spoofing, occurs when a hacker inside or outside a network impersonates a trusted computer.

Call Interception is the unauthorized monitoring of voice packets or RTCP transmissions. Hackers could capture the packets and decode their voice packet payload as they traverse a

large network. This kind of attack is the equivalent of wiretapping in a circuit-switched telephone system.
Repudiation attacks can take place when two parties talk over the phone and later on one party denies that the conversation occurred.
Call Hijacking or Redirect attacks could replace a voice mail address with a hacker-specified IP address, opening a channel to the hacker [Gre04]. In this way, all calls placed over the VoIP network will fail to reach the end user.
Denial-of-service (DoS) attacks prevent legitimate users of a network from accessing the features and services provided by the network.
Signal protocol tampering occurs when a malicious user can monitor and capture the packets that set up the call. By doing so, that user could manipulate fields in the data stream and make VoIP calls without using a VoIP phone [Pog03]. The malicious user could also make an expensive call, and mislead the IP-PBX into believing that it was originated from another user.
Attacks against Softphones occur because as they reside in the data VLAN, they require open access to the voice VLAN in order to access call control, place calls to IP phones, and leave voice messages. Therefore, the deployment of Softphones provides a path for attacks against the voice VLAN. VoIP systems are capable of handling large volumes of calls using both IP phones and Softphones. Unlike traditional phones, which must be hardwired to a specific PBX port, IP phones can be plugged into any Ethernet jack and assigned an IP address. These features not only represent advantages but also they may make them targets of security attacks.
Note that all these attacks apply also to conference calls and some may apply to the use of voice mail.

2.2 Registration attacks

Brute Force attacks are simply an attempt to try all possible values when attempting to authenticate with a system or crack the crypto key used to create ciphertext [Bre99]. For example, an attacker may attempt to brute-force attack a Telnet login, he must first obtain the Telnet prompt on a system. When connection is made to the Telnet port, the hacker will try every potential word or phrase to come up with a possible password.
Reflection attacks are specifically aimed at SIP systems. It may happen when using http digest authentication (i.e. challenge-response with a shared secret) for both request and response. If the same shared secret is used in both directions, an attacker can obtain credentials by reflecting a challenge in a response back in request. This attack can be eliminated by using different shared secrets in each direction. This kind of attack is not a problem when PGP is used for authentication [Mar01].
The *IP Spoofing* attacks described earlier can also be classified as registration attacks.

2.3 Attacks against Audit (IP-PBX and operating systems)

Due to their critical role in providing voice service and the complexity of the software running on them, IP PBXs are the primary target for attackers. Some of their vulnerabilities include:

- *Operating system attack.* Exploits a vulnerability in an operating system. An attack that makes use of this vulnerability, while perhaps not directed toward a VoIP system, can nevertheless create issues.

- *Support software attack.* Exploits a vulnerability in a key supporting software system, such as a database or web server. An example is the SQL Slammer worm, which exploited a vulnerability in the database used on a specific IP PBX.
- *Protocol attack.* Exploits a vulnerability in a protocol implementation, such as SIP or H.323. An example is the vulnerability in the H.323 implementation in Microsoft's ISA Server.
- *Application attack.* Exploits a vulnerability in the underlying voice application, which is not filtered by the protocol implementation.
- *Application manipulation.* Exploits a weakness in security, such as weak authentication or poor configuration, to allow abuse of the voice service. For example, registration hijacking or toll fraud.
- *Unauthorized access.* Occurs when an attacker obtains administrative access to the IP PBX.
- *Denial of Service.* Either an implementation flaw that results in loss of function or a flood of requests that overwhelms the IP PBX [Col04].

3. Network forensic challenges

3.1 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 comprehensive and more oriented to our research approach. 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 synchronization	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 preservation phase involves acquiring, seizing, and securing the digital evidence; making forensic images of the evidence; and establishing the chain of custody. The middle phases of the forensic process (i.e., the collection, examination, and analysis of the evidence) provide network investigators with a 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.
We concentrate on the initial phase of the forensic process, the identification of potential digital evidence (i.e., where the evidence might be found), which is flagged by IDS and, in some sense, by the attack patterns.

3.2 VoIP Evidence Collector

The VoIP Evidence Collector pattern [Pel10] 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.

3.2.1 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.

3.2.2 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].

3.2.3 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.

3.2.4 Structure

Figure 2 shows a UML class diagram describing how a VoIP evidence collector [Pel10] and an IDS system integrate. The evidence collector is attached to hosts or network components (e.g. call server) 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 Network Forensic Analysis Tools (NFAT). VoIP components that are monitored can provide forensics information once an attack occurs. The Evidence Collector is designed to extract forensic data and securely transport it (i.e., hash and encrypt) to a forensic server using a VoIP secure channel [Fer07]. 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.

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.

3.2.5 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.

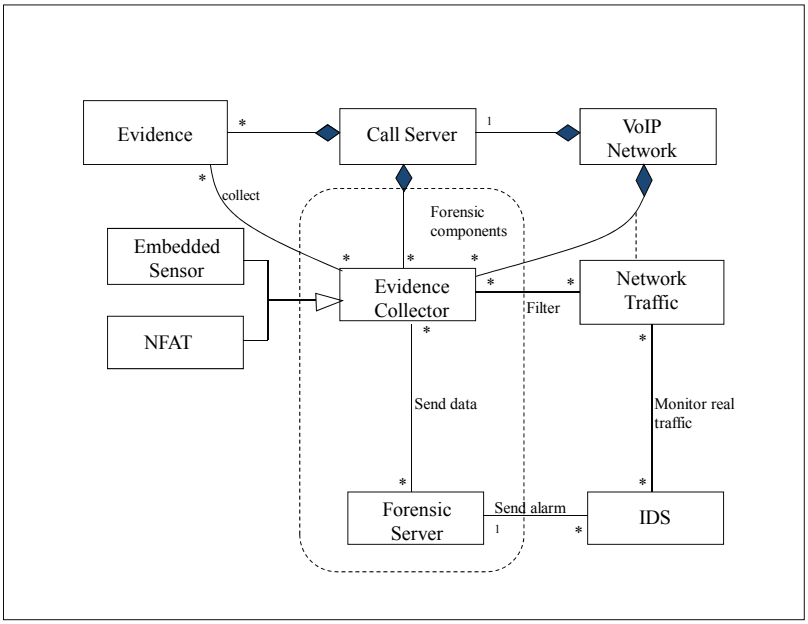


Fig. 2. Evidence Collector Class Diagram

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 [Fer07] to monitor the voice VLAN traffic independently from data VLAN traffic although the two share the same converged network.

3.2.6 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.

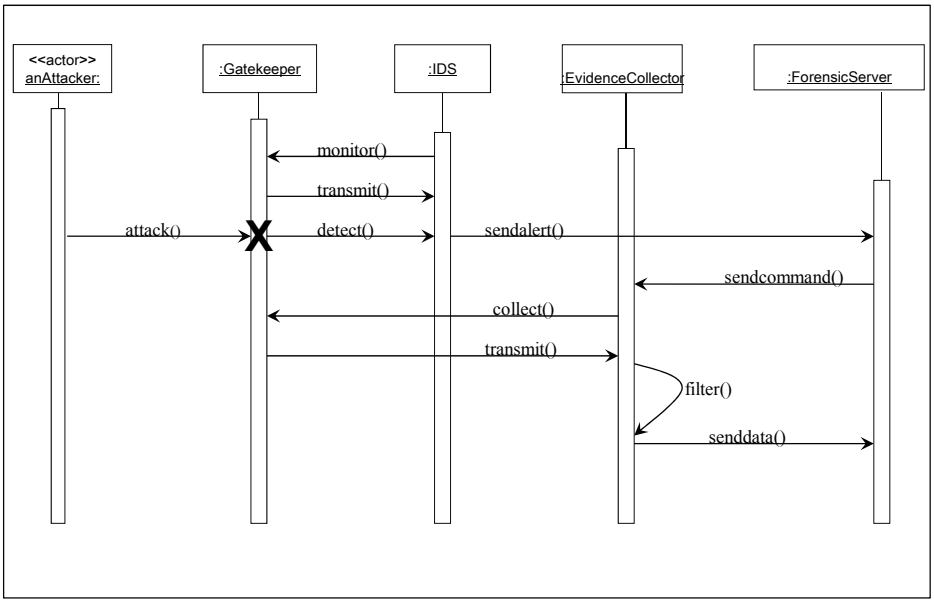


Fig. 3. Evidence Collector Sequence Diagram

3.2.7 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].

4. Protocol anomaly detection

Protocol anomaly detection is based on models characterizing proper use of protocols, and any behavior that departs from the model will be regarded as intrusive or suspicious. In this approach, protocols are well defined, and a normal use model can be created with greater accuracy [Aln08]. The creation of a complete profile of normal network traffic that implements a particular protocol is the core of this protocol behavior detection method. The SIP protocol has specific features that show a sequence of finite states that specify the correct behavior in a VoIP network.

A protocol-based IDS method is able to detect attacks against the converged network using information collected from both signaling and media packets. This method focuses on detecting misuse of the protocol's vulnerabilities. In this technique, the system detects attacks using information that is collected from the protocol headers.

4.1 Technical approach

The protocol-based detection technique defines a structure and demonstrates a process for collecting VoIP attack packets on the basis of adaptively setting filtering rules for real-time collection. The collected data is sent to a network forensics analyzer for further analysis. This data is used to discover and reconstruct attacking behaviors.

In our approach, we used an IDS infrastructure to collect details about attacker activities against VoIP components (e.g., gatekeeper) and the voice packets on the network. The IDS framework is a distributed attack sensing and warning system that uses a series of network-based collection sensors to acquire relevant forensic information so that intrusion analysts can perform effective analysis. This system has been designed to enable high

interoperability between tools used for performing network traffic analysis. It achieves this by storing all collected traffic in a central repository and allowing the analysis tools to run on the collected data. This eases the burden on the sensors (machines used for collecting traffic) by making them simple collection agents.
In VoIP forensic investigations, these devices will be deployed in a converged environment, thus reducing human intervention. These hardware devices will be attached in front of the target servers (e.g., call server) or sensitive VoIP components in order to capture all voice packets entering or leaving the system. These sensors will also be used by the IDS to monitor the VoIP network.
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 selected voice packets (i.e., request or response) over the VoIP network by applying a filter. The data collected by the evidence collectors is stored in a storage area network cluster and will be used to perform the corresponding forensics analysis. We can also use network segmentation techniques [Fer07] to monitor the voice virtual local area network (VLAN) traffic independently from data VLAN traffic, although the two share the same converged network.

4.2 Structure

Figure 4 shows the UML class diagram of the specification-based IDS approach. This diagram generalizes the intrusion detection process in a VoIP call and shows the caller and callee roles. The model shows how it becomes possible to intercept an access request for a VoIP service. The IDS system uses an attack detector to match the sequence of message requests to the profiles in the user profile set and decides whether the request is an intrusion or not. If an attack is detected, some countermeasures that guarantee to maintain the confidentiality, authenticity, integrity and nonrepudiation of the entire VoIP infrastructure are performed.

4.3 Dynamics

The sequence diagram in figure 5 shows the necessary steps for profile matching when an attack access request has been made using VoIP technology. When the IDS detects any attempt to use the VoIP service without authorization or a known attack against VoIP components, it gives alarms to the system, which in turn blocks the call request through a firewall.

5. Dimensionality reduction and statistical methods for intrusion detection

Dimensionality reduction methods allow detection and estimation in a manifold of smaller dimension than the data stream. This improves the speed of detection and greatly reduces the complexity of the algorithms without compromising performance.
Dimensionality reduction methods have been applied in various domains, such as face recognition and information retrieval systems, to drastically reduce computational costs of processing high-dimensional data via the generation of a low-dimensional feature space that preserves relevant aspects of the data. Dimensionality reduction-based alternative methods use statistical signal processing methods in VoIP networks.
Our method for dimensionality reduction is based on linear random projections. Based on the isometry properties of random matrices and the Johnson-Lindenstrauss lemma, it can be

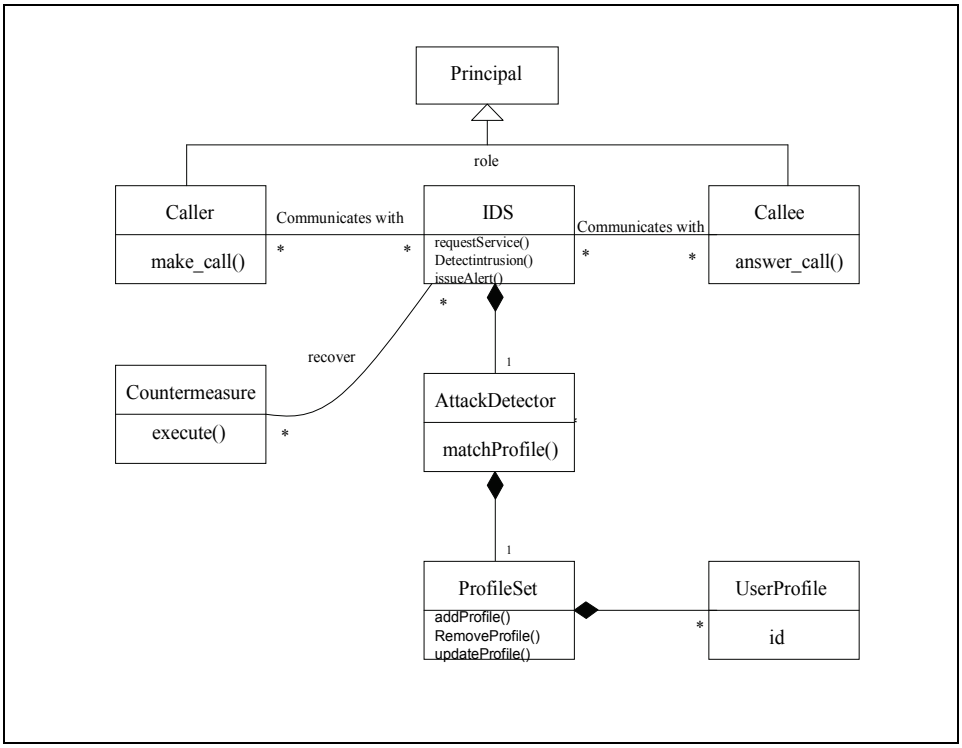


Fig. 4. Class diagram for a specification-based IDS

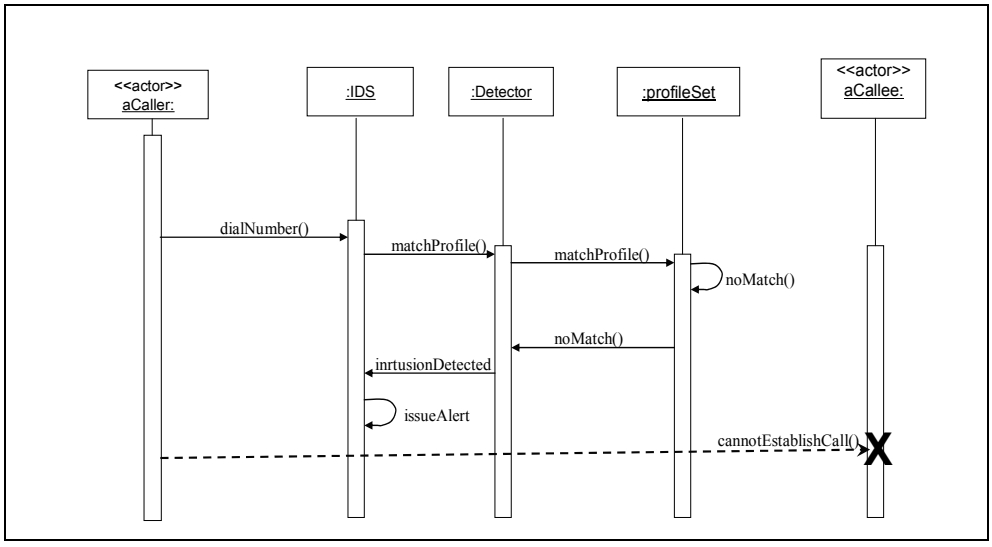


Fig. 5. Sequence diagram for detecting VoIP attacks

demonstrated that dimensionality reduction by random projections preserves the local topology of sparse signal spaces [Don06]. Moreover, if prior information about the normal signal space is known, subspace random projections can be used to further improve the accuracy of detection and separation of the different classes of anomalies [Par09, Wan10]. The incorporation of readily used techniques like Self Organizing Maps and Support Vector machines over projected data samples showing very good results over *randomly* projected data [Arr06, Cal09] are evaluated as well.
The main goal is to develop algorithms to detect and classify anomalies using compressed versions of the original traffic data and possibly learn the different classes of anomalies from live traffic. We expect that this approach will improve the speed of detection and greatly reduce the complexity of the algorithms without compromising performance.

5.1 Technical approach

Dimensionality reduction and statistical methods are used to identify threats in VoIP networks. The proposed intrusion detection system approach provides real-time network intrusion detection by projecting the high dimensional dataset to a lower dimensional space using the random projection technique, then performing intrusion detection in the lower dimensional space using statistical detection methods.
To that end, processing data is separated in two stages. The first stage consists of mapping packets to vectors in a Euclidean space and the subsequent dimensionality reduction. The second stage consists of learning different classes of anomalies and classifying incoming data. A key assumption for the success of the proposed system is the possibility to isolate the anomalies from the underlying normal traffic structure. The algorithms used in this approach model the normal traffic data as part of a manifold or subspace. If this assumption holds for the kind of traffic involved in VoIP communications, then the base of the subspace or the parameterization of the manifold can be used to isolate and filter the normal traffic contributions to the observed traffic prior to compression.
After performing the mapping, subspace random projections are used to jointly reduce and filter the observed vector. The vector corresponding to the payloads and the vector corresponding to the headers are analyzed separately, and a decision is made about the nature of the block of packets using the information extracted from both vectors.

5.1.1 Classification through compressive measurements

If we consider the stream of bits from the RTP, SIP, or RTCP packets as an N-dimensional vector of great dimension, we can solve the problem of anomaly detection from the projections of the data vector in a proper random basis. The idea is to classify all the normal patterns in the compressed domain and then detect the presence of anomalies by contrasting with the typical set elements. In general many problems of classification or detection can be solved directly in the compressed domain as explained in [Dav09]. A particular capability that will be sought is that of reconstructing the original packets from dimensionally reduced samples if traffic is presumed malicious. Part of our research will be to adapt this method to the framework of stream detection and classification of data streams. Detecting intrusions in the projected lower dimension reduces the complexity of the underlying algorithms, which makes it more suitable for real time detection. Moreover, lower dimensional data can be stored and transmitted more efficiently than its higher dimensional data, thereby saving system resources.

Classification algorithm demands repeated computation of similarity between pairs of vectors and the computational overhead increases with the increase in the dimensionality of the vectors. We consider that dimensionality reduction of these vectors will help in classification, reduce the processing time, and improve the efficiency of the IDS. However, the choice of dimensionality reduction method critically depends on preservation of similarity for efficient classification. In our approach we use the compress sensing theory, which states that with high probability, every K-sparse signal $x \in RN$ can be recovered from just $M=O(K.log(N/K))$ linear measurements $y=\Phi.x$, where Φ represents an M×N measurement matrix drawn randomly from an acceptable distribution [Don06]. Therefore, to classify input vectors we use machine learning algorithms such as support vector machines (SVM) and self- organizing maps (SOM).

5.1.2 Stream entropy estimation

A characterization in terms of stream entropy and sequence typicality of the different sections of the RTP, SIP, and RTCP flows is performed to identify and classify normal and potentially malicious traffic flows. Our approach is to use information theoretic measurements of the protocol headers to reveal the presence of higher-than-normal, sustained variation indicative of a covert channel. The entropy estimation is carried out through sparse sampling of the data stream. By the bounds given in [Lal06] for sparse sampling, one can assure that the estimation of the entropy will be within a fixed error margin of the actual value obtaining good levels of accuracy and with a reduced number of measurements and memory space required.

Dimensionality reduction methods based on spectral properties of a data matrix are attractive for application to entropy detection; spectral dimensionality reduction methods include principle components analysis, linear discriminant analysis, and singular value decomposition [Ski07]. These methods have strong statistical foundations, and are provably optimal for preserving variance of a dataset. Therefore, it is expected that they will likewise be optimal for preserving entropy. Application of these methods to entropy computation for network intrusion detection is not completely straightforward, because one must either choose a static feature subspace in which to compute entropy or continually generate new feature subspaces.

6. Converged experimentation testbed

The objective of this testbed is to evaluate developed algorithms in a systematic manner, and to evaluate the state of the art open source, COTS, and GOTS tools to determine holes for focusing future research initiatives. Technically, this task involves the development of simulation components for different signaling protocols, audio and video transports, and codecs. The testbed supports both the generation of normal (real and simulated) VoIP traffic.

This testbed is also used to verify the performance of the stream entropy-based intrusion detection scheme with network attack experiments. The converged testbed supports the generation of normal (real and simulated) VoIP traffic to compute the distribution of baseline stream under normal conditions. The performance of the IP telephony IDS is evaluated with two metrics: detection rate and false-positive alarms.

7. Conclusions and future work

For the purpose of intrusion detection in VoIP, our approach is based on stream entropy estimation, second order statistics, and dimensionality reduction. Entropy-based feature spaces have been shown to be successful for detecting network anomalies. Unfortunately, entropy detection is computationally expensive; indeed, parallel methods have been proposed to allow for more scalable entropy computation. A very scalable alternative to distributed entropy computation is computation of entropy in a compressed domain via dimensionality reduction.

We have run the proposed algorithm against both data transmitted and stored in our IDS database where the tool was successful at detecting attack packets with very high accuracy. Upon integration into IDS infrastructures, we expect this forensic tool will enable a faster response and more structured investigations of VoIP-based network attacks.

The use of dimensionality reduction methods for intrusion detection is a promising direction. The exploration of dimensionality reduction and related statistical approaches will allow network analysts to better understand more complex aspects of intrusion detection in converged environments. These technologies will primarily be targeted toward applications and techniques that capitalize on a distributed attack sensing and warning system.

The approach should be helpful to network analysts for identifying and understanding the mechanisms needed to efficiently detect attacks in converged systems. When encryption is present, the detection tool can capture the headers and contents of packets separately.

Future work will include the design of a structure and process to analyze the collected VoIP forensic data packets. This will allow the detection of attacks against the converged network using information collected from VoIP protocol headers. Future work will also include the creation of a misuse pattern catalog containing a set of all attack patterns we want to capture.

8. References

[Aln08] Al-Nashif, Y.; Hariri, S.; Luo, Y.; Szidarovsky F. Autonomic Intrusion Protection System (AIPS). *IEEE Transactions on Computers* 2008, *6*.

[Arr06] R. Arriaga, and S. Vempala. "An algorithmic theory of learning: Robust concepts and random projection" Machine Learning, Number 2, Volume 63, pages 161-182, 2006

[Bre99] C. Brenton. "Mastering Network Security," Network Press, San Francisco, 1999

[Cal09] R. Calderbank, S. Jafarpour, and R. Schapire. "Compressed learning: Universal sparse dimensionality reduction and learning in the measurement domain", http://dsp. rice.edu/files/cs/cl.pdf, 2009

[Col04] M. Collier. "The Value of VoIP Security", July 2004. http://www.voipsecurityblog.typepad.com/

[Dav09] M. Davenport, M. Wakin, and R. Baraniuk, "Detection and estimation with compressive measurements," *Dept. of ECE, Rice University, Tech. Rep*, 2006.

[DFRWS01] Digital Forensics Research Workshop. A Road Map for Digital Forensics Research 2001. *Digital Forensics Research Workshop 6 November* (2001): http://www.dfrws.org.

[Don06] D. L. Donoho ," Compressed sensing" IEEE Transactions on Information Theory, Number 4,Volume 52, pages 1289—1306 , 2006

[Fer05] Fernandez, E. B.; Kumar, A. A Security Pattern for Rule-Based Intrusion Detection, *Proceedings of the Nordic Pattern Languages of Programs Conference*, Otaniemi, Finland, September 23–25, 2005; Viking PLoP, 2005.

[Fer06] E. B. Fernandez, M.M. Larrondo-Petrie, T. Sorgente, and M. Van-Hilst, "A methodology to develop secure systems using patterns", Chapter 5 in "Integrating security and software engineering: Advances and future vision", H. Mouratidis and P. Giorgini (Eds.), IDEA Press, 2006, 107-126.

[Fer07] Fernandez, E. B; Pelaez, J. C.; Larrondo-Petrie; M. M. Security Patterns for Voice Over IP Networks. *Proceedings of the 2nd IEEE International Multiconference on Computing in the Global Information Technology* (ICCGI 2007), March 4–9, 2007, Guadeloupe, French Caribbean.

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

[Gree04] D. Greenfield, "Securing The IP Telephony Perimeter", April 5,2004. http://www.networkmagazine.com/shared/article/showArticle.jhtml?articleId=18900070

[Ken06] Kent, K.; Chevalier, S.; Grance, T.; Dang, H. Guide to Integrating Forensic Techniques into Incident Response. National Institute of Standards and Technology, *NIST Special Publication 800-86*, August 2006.

[Lal06] A. Lall, V. Sekar, M. Ogihara, J. Xu, H. Zhang. "*Data Streaming Algorithms for Estimating Entropy of Network Traffic.*" IN ACM SIGMETRICS, p 145-156, 2006.

[Mar01] M. Marjalaakso. "Security requirements and Constraints of VoIP." September 17 2001. http://www.hut.fi/~mmarjala/voip

[Par09] J. Paredes, Z. Wang, G. Arce, and B. Sadler. "Compressive Matched Subspace Detection" European Signal Processing Conf. 2009.

[Pel09] J.C. Pelaez. "Using Misuse Patterns for VoIP Steganalysis." *Proceedings of the Third International Conference on Secure Systems Methodologies Using Patterns (SPattern'09).* Linz, Austria, August 31- September 04, 2009.

[Pel10] J.C. Pelaez and E.B. Fernandez. "VoIP Network Forensic Patterns." International Journal on Advances in Security. http://www.iariajournals.org/security/index.html.

[Pog03] J. Pogar. "Data Security in a Converged Network" July 23, 2003 http://www.computerworld.com/securitytopics/security/story/0,10801,83107,00.html

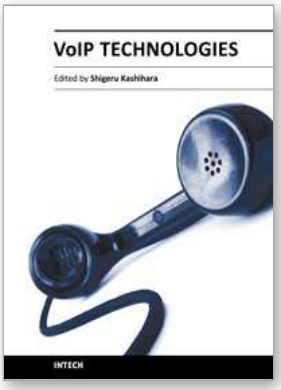
[Ren05] W. Ren, H. Jin. "Distributed Agent-based Real Time Network Intrusion Forensics System Architecture Design." *Proceedings of the 19th International Conference on Advanced Information Networking and Applications* (AINA'05). March, 2005.

[Ski07] D. Skillicorn. "Understanding Complex Data Sets: Data Mining with Matrix Decompositions." Chapman and Hall, Boca Raton, FL, USA, 2007.

[Sta02] W. Stallings. "Network Security Essentials: Applications and standards." Prentice Hall, Upper Saddle River, 2002, 5 – 21

[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.

[Wan10] Z. Wang, J.L Paredes and G. R. Arce "Adaptive Subspace Compressed Detection of Sparse Signals" submitted for publication , 2010.



VoIP Technologies

Edited by Dr Shigeru Kashihara

ISBN 978-953-307-549-5
Hard cover, 336 pages
Publisher InTech
Published online 14, February, 2011
Published in print edition February, 2011

This book provides a collection of 15 excellent studies of Voice over IP (VoIP) technologies. While VoIP is undoubtedly a powerful and innovative communication tool for everyone, voice communication over the Internet is inherently less reliable than the public switched telephone network, because the Internet functions as a best-effort network without Quality of Service guarantee and voice data cannot be retransmitted. This book introduces research strategies that address various issues with the aim of enhancing VoIP quality. We hope that you will enjoy reading these diverse studies, and that the book will provide you with a lot of useful information about current VoIP technology research.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821