

A method for forensic artifact collection, analysis and incident response in environments running Session Initiation Protocol (SIP) and Session Description Protocol (SDP)

Vasilios Katos¹, Ioannis Psaroudakis¹, Panagiotis Saragiotis¹ and Lilian Mitrou²,

¹ Dep. of Electrical and Computer Engineering

Democritus University of Thrace

University Campus, Kimmeria, Xanthi 67100, Greece

² Dep. of Information and Communication Systems Engineering

University of the Aegean

Karlovassi GR-83200, Samos, Greece

{vkatos, psaroudakis}@ee.duth.gr, l.mitrou@aegean.gr

Abstract

In this paper we perform an analysis of SIP, a popular Voice over IP (VoIP) protocol and propose a framework for capturing and analyzing volatile VoIP data in order to determine forensic readiness requirements for effectively identifying an attacker. The analysis was performed on real attack data and the findings were encouraging. It seems that if appropriate forensic readiness processes and controls are in place, a wealth of evidence can be obtained. The type of the end user equipment of the internal users, the private IP, the software that is used can help build a reliable baseline information database. On the other hand the private IP addresses of the potential attacker even during the presence of NAT services, as well as and the attack tools employed by the malicious parties are logged for further analysis.

Keywords: *Network forensics, SIP, VoIP Forensics, Intrusion Detection Systems (IDS)*

1 Introduction and motivation

Voice over Internet Protocol (VoIP) is a prevailing technology allowing users to place phone calls over the Internet and eventually to replace traditional time division multiplexing (TDM) telephony. According to market predictions (Infonetics, 2012) in the next five years over \$377 billion are to be invested on VoIP and Unified Communication (UC) services.

SIP and the H.323 protocol suite are currently the two prevailing standards offered to develop a VoIP service. SIP has been developed and supported by the Internet community whereas the H.323 has been developed by the telecommunication companies. Of the two protocols, SIP is the preferred solution for connecting end user equipment whereas H.323 is primarily used in the interconnection of the telephony switches and in video conference systems. It is worth noting of Skype service in Internet telephony due to the large market share it maintains, involving a proprietary technology run by a single company.

A number of vulnerabilities have been identified for VoIP (Keromytis, 2010) and it seems that existing and traditional security controls and solutions like firewalls and IPSec cannot fully address them as VoIP operate on heterogeneous environments (Walsh and Kuhn 2005) which are in principle challenging to secure. The common VoIP security threats involve (Dwivedi 2009):

- VoIP sniffing
- VoIP Phishing
- Making Free Calls
- Caller ID Spoofing
- Anonymous Eavesdropping and Call Redirection
- Spam Over Internet Telephony (Gritzalis et al., 2013)

The relatively wide adoption of VoIP by a large user base combined with its vulnerabilities has inevitably resulted to making such infrastructures appealing also to criminals. For example, organized crime may sniff a judge's unencrypted Internet phone call and use it for blackmailing purposes. Moreover, organized crime has the ability to set up and operate private telecommunication services outside the realms of official telephony providers. It is quite difficult for law enforcement

authorities to trace this kind of phone calls because in most cases they are unaware of their existence and furthermore it can be more difficult and challenging to collect valuable and reliable evidence.

Network forensics is an aspect of digital forensics dealing with monitoring and analyzing network traffic aiming to collect information and find evidence of illegal activity. Evidence can also be found in routers' routing tables, in Content Addressable Memory (CAM) memory of switches, in firewall logs, in DHCP server logs, in web proxy logs, in intrusion detection systems logs and in authentication services logs (Davidoff 2012). Most of these pieces of evidence are volatile and change dynamically. For example the default value of the ARP table timeout in a Cisco switch is set to expire after four hours. Therefore a network forensic procedure must run proactively in a computer network in order to promote forensic readiness. However we should also acknowledge issues surrounding proactive collection of evidence as such practice hardly complies with the existing legislations.

This paper focuses on artifacts that can be collected in a VoIP service and especially in the SIP headers and the SIP body message where the SDP data lie. SDP is used "to convey media details, transport addresses, and other session description metadata to the participants during an Internet call" (RFC4566, p.2). SDP contains information in its headers that is of a particular forensic value, as it includes the private IP address of the User Agent. Private IP address should be used by intermediate devices between the SIP server and the User Agent such as firewalls or routers in order to dynamically build and preserve the Network Translation Table (NAT) reinsuring bidirectional communication. When intermediate devices do not process these headers (either being incapable or not configured accordingly), private IP address may reach the remote SIP server thus leaking information of a private network topology. Apart from the private IP addresses, other useful artifacts can be collected from these headers most of which are not logged by the SIP servers as it was confirmed during the empirical evaluation of this work.

This paper is structured as follows. Section 2 presents a brief review of the existing literature on VoIP forensics. In Section 3 the relevant and worth preserving artifacts found in SIP and SDP headers in respective request and response methods are presented. We also describe the framework for the packet capture and analysis. Section 4 contains the empirical evaluation and results followed by a comparison of the proposed method related with server logging and IDS. Legislation compliance is examined in Section 5. Finally Section 6 summarizes the conclusions and propositions for future work.

2 Related Work

VoIP forensics is a relatively new research area in network forensics. Researchers, law enforcement authorities and digital investigators have proposed methods and developed techniques in an effort to collect and handle the digital evidence pertaining to VoIP activities. Simon and Slay (2006) propose the so-called 4Ps model, comprising of Prevention (firewalls, IDS/IPS etc), Protection (encryption, security management, etc), Preservation (logs, records and analysis) and Presentation (Vulnerability management and repair mechanisms). Lin and Yen (2011) further expanded the 4Ps model and have adjusted it to meet VoIP needs in a detailed forensics procedure called the VoIP DEFSOP (Digital Evidence Forensics Standard Operating Procedure). The Preservation stage is now mapped to the Operational Stage and is further expanded to the Collection, Analysis and Forensics stages. A technical limitation of this model is that when implemented it requires deployment of agents on all participating nodes (both clients and server) in order to collect the data, which in some cases may not be practically feasible as clients may not always reside under the same management domain with the servers and furthermore there may be proprietary or embedded devices (such as hardware SIP phones) with no option to install additional software. Such limitation needs to be addressed in future solutions and is a requirement for the work proposed in this paper. Yen et al. (2011) present a case study based on VoIP DEFSOP but similar to the above, the collection of data requires local acquisition and special requirements to be met such as prior installation of specific software to both the server and the clients.

Hsu et al. (2011) describe a collaborative scheme for VoIP traceback. VoIP traceback is a challenging task because artifacts are geographically distributed in different places between clients, servers and network equipment that are managed by different administrators, or even worse, by different organizations. As such, in a scenario where a user resides in a private network, the private IP would need to be requested from the remote network operator. In our proposed work it is demonstrated that this information can be obtained by mining the SDP headers which can be collected locally, without the need for network operator collaboration thus saving on administrative overheads.

Irwin and Slay (2011) developed an application that searches for VoIP artifacts in the computer's volatile memory. They showed that Real-Time Transport Protocol (RTP) conversations can be reconstructed with a significant probability of success from the data residing in RAM. This approach can significantly augment and complement our proposed method. Psaroudakis et al. (2012) demonstrated that in case of a smartphone VoIP client the User Agent header can lead to full disclosure of a smartphone's make, model, and operating system. This has also been verified in the present work for a number of legitimate users. François et al. (2010) proposed a method for fingerprinting the SIP User Agent. This method could contribute to an effort to discover spoofed SIP User Agents headers from malicious users. In our case study it was discovered that a portion of malicious users attempted to hide their identities and details of the attacks by spoofing their User Agent header.

3 SIP (forensic) acquisition and analysis framework

SIP and SDP are used as a signalling protocol for the audio/video stream used during a VoIP call. The actual voice/video data are transmitted by the RTP. Since it is unlawful to intercept a voice call without a warrant we exclude monitoring, processing and analysis of the RTP packets. We consider that the logging and the preservation of the signalling data as a legal action according to the Data Retention Directive. Such assumption is similar to logging email metadata, rather than the actual email contents. However the processing and analysis of the preserved data has some barriers which are derived by the respective legislation. The latter is examined in the last section of this work.

The framework (Fig. 1) consists of four main components:

- the data collecting process which collects the SIP packets from the data network;
- the SIP artifacts forming process which is achieved through database mining;
- the user's malicious activity detection process, and
- the correlation process.

3.1.1 Collection Process

The collection process involves an acquisition stage that continuously collects the network traffic. The placement of the network capture server is of great importance. The "tap" must be able to sniff all the traffic of a given network. Therefore the network capture must be placed behind the border router or the main firewall of the network.

The application running on the capture server filters the appropriate SIP and SDP headers of preselected SIP methods. These filtered data are then stored in a database. The application that collects the network traffic, filters it and stores it in the database is called the *parser*.

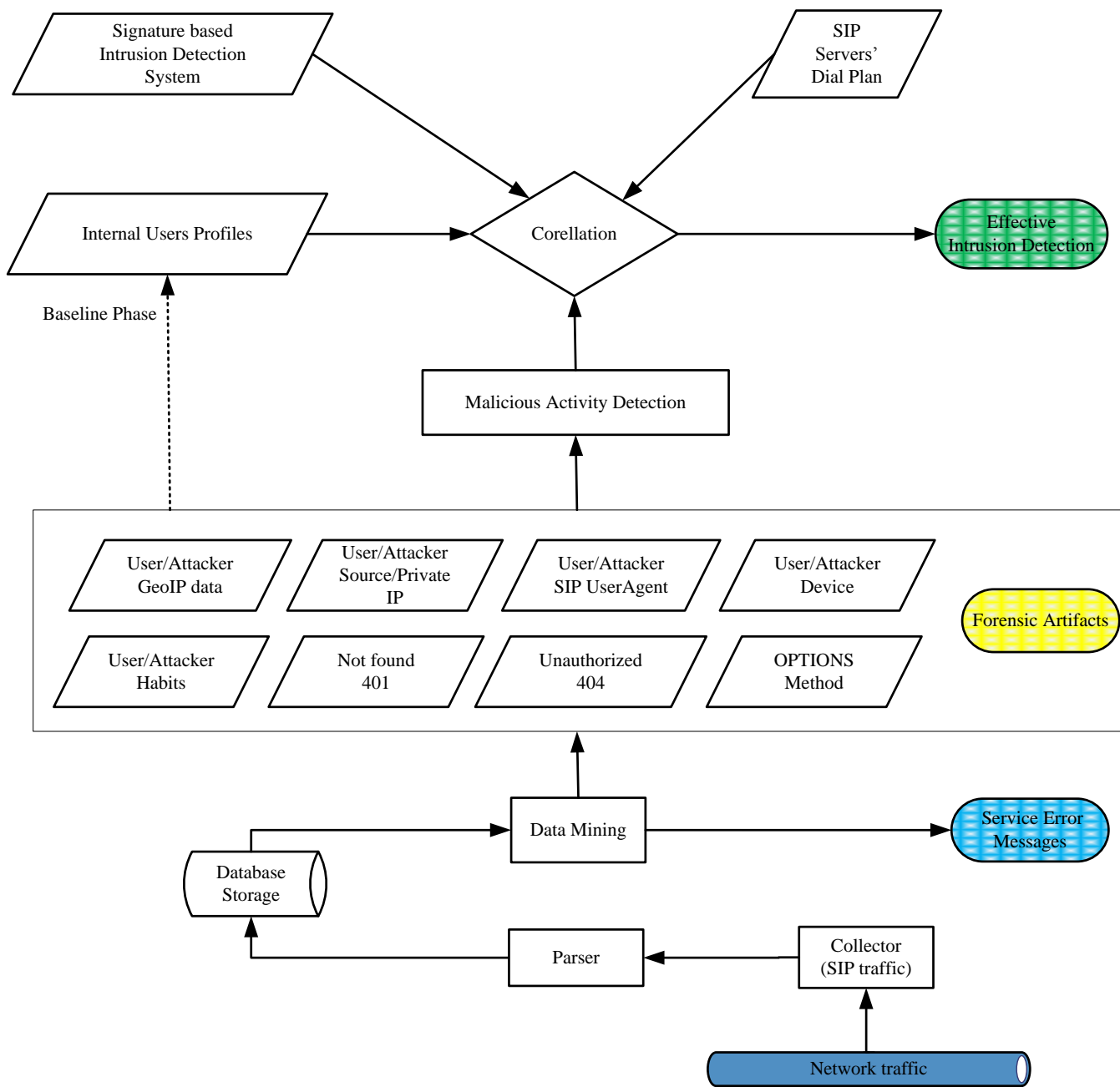


Figure 1: SIP (forensic) acquisition and analysis framework

3.1.2 Forming Forensic Artifacts in SIP/SDP

Both SIP and SDP contain a wealth of headers. After following a thorough selection process, we concluded with a subset of headers and SIP methods that provide us with the valuable forensic evidence with low volume data fingerprint. In Table 1 we briefly describe these headers with their respective operation inside the protocol. Alongside we present the forensic relevance of these artifacts. Through database mining in headers values and the SIP methods we build the forensic artifacts.

Field	Description (RFC 3261, 2002)	Artifacts
Frame Time	Universal Time Clock of captured frame	By using Network Time Protocol (NTP) on the server that captures the packets we reinsure the proper logging time of the incident.
Source IP	Source IP address as extracted from IP	Source IP address derived from IP packet that is harder to

address	packet.	spoof.
Destination IP Address	Destination IP address as extracted from IP packet.	Destination IP address derived from IP packet that belongs to a local monitored SIP server.
SIP From	The "From" header field indicates the logical identity of the initiator of the request, possibly the user's address-of-record. It contains a Uniform Resource Identifier (URI) and optionally a display name	In the case of a request originating from a legitimate user of the service this header is expected to contain a legitimate and valid URI of a monitored SIP server. In case of an attack this header usually contains a spoofed URI.
SIP Contact	The "Contact" header field contains the URI at which the User Agent would like to receive requests, and this URI must be valid even if used in subsequent requests outside of any dialogs.	In case of a legitimate request we expect in this header a legitimate URI. Some User Agents report their private IP in this field along with the public IP.
SIP To	The "To" header field first and foremost specifies the desired "logical" recipient of the request, or the address-of-record of the user or resource that is the target of this request.	The conclusions we can derive from the "To" header depend on how the monitored SIP server is setup. A SIP server may allow calls only between internal users or it may be programmed to allow calls to foreign (national or international) destination numbers. If a SIP server constantly receives requests to an international number while it is programmed only for internal calling, then we have a very strong indication of a Free Call Attack.
SIP User Agent	The client agent who deals the communication.	Useful information is revealed in User Agent header that is not logged by the servers we used for evaluation. We can record the name of the software used (softphone) and we may also derive information about the operating system. We can record the make, model or even firmware version in case a SIP phone used. Especially in softphones used in modern smartphones except for the application name we can derive information about the make and model of the smartphone itself. In case of an attack this field will contain either a string of random characters or the name of the tool used (i.e. SipCli).
Via	Shows the transport protocol used and the request route, each proxy adds a line.	By examining the "Via" header we may discover an incoming request through an intermediate proxy.
Call-Id	Unique identifier for each call which contains the host address. It must be the same for all the messages within a transaction.	This is the identification string of each call and can be useful when tracing a call between SIP proxies.
Cseq:	Cseq begins with a random number and it identifies in a sequential way each message.	The "Cseq" header is used to trace the reply message from the SIP server for each request we monitor, as SIP runs over UDP which is stateless.
SDP Owner	This field gives the originator of the session (her username and the address of the user's host) plus a session identifier and a version number.	The "SDP Owner" header contains information about the remote user and the remote IP address. In case of a legitimate user this IP is the same with the source IP or the private IP of the remote host if it is connected through NAT. In case of an attack it is usually spoofed (it seems to depend on the attacking tool used).
SDP Connection	This field contains connection data. A session description MUST contain either at least one "c=" field in each media description or a single "c=" field at the session level.	This header contains the IP address of the requesting peer.
Field	Description (RFC 3261, 2002)	Artifacts
SDP Session Name	This field is the textual session name.	This header is usually named after the application in case of softphone. In case of an attack it is usually left blank.
SDP Media Attributes	Attributes are the primary means for extending SDP. Attributes may be defined	In "SDP Media Attributes" we can find information about audio codec capabilities of the remote host. It is worth

	to be used as "session-level" attributes, "media-level" attributes, or both.	mentioning that in this field we can also find the private IP of the remote host when it is connected through NAT. In one case we discovered three private IPs of the remote host. In some attacks we found this field being spoofed. In some other attacks private IP of the remote attacker was revealed.
Info Request (wireshark ¹)	n/a	This field is generated by the popular wireshark packet analyzer application. It provides brief information about each packet captured relating to the underlying application. In our case, this field provides information relating to the SIP context, so we are informed of the SIP methods used for each transaction.
Info Response (wireshark)	n/a	Similar to the above, but for the respective response.

Table 1: Valuable artifacts in SIP/SDP headers and primary empirical findings

3.2 SIP Methods Requests and Responses

The SIP protocol uses request methods originating from the caller in order to establish a call session. The callee responds to the specific request with a corresponding response code. There are fourteen SIP request methods and six classes of response codes. From a forensics perspective we examine the packets containing request methods like "INVITE", "REGISTER", "SUBSCRIBE" and "OPTIONS". The SIP response codes of the 4xx class and 2xx class with session description class are also examined.

3.2.1 INVITE / REGISTER Requests

The INVITE method request indicates that a SIP User-Agent is being invited to participate in a call session (RFC 3261). A typical successful SIP transaction during an INVITE negotiation is illustrated in Fig.1. The remote user (denoted as the smartphone icon) is eligible (authenticated, in access list, etc.) for placing a call and received a "Status 200 OK" response code. The same applies during a successful REGISTER request. The REGISTER method registers the SIP User-Agent's address (that is listed in the To header field) with a SIP server (RFC3261).

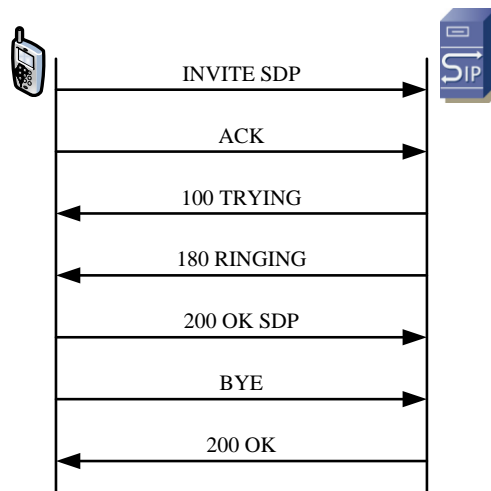


Figure 2: SIP INVITE negotiation

From a forensics perspective, during the SIP INVITE and the SIP REGISTER requests a great wealth of information is revealed. For a given user we can find the source IP of the remote host, the User Agent application, the Caller ID that a user has set to his application, the calling party and sometimes even the private IP hidden behind a NAT. Depending on the User Agent software employed, the private IP address can be found in various headers and differing locations, as there seems to be no standard approach of imprinting the IP addresses in the SIP headers. Recording the private IP address can significantly help investigators resolve a case when the incident occurs behind a NAT server.

¹ Wireshark is a popular open source network analyzer application.

From the empirical experiment it was also confirmed that some applications report their private IP address during the **REGISTER** process in the SIP Via and/or the SIP Contact Header

Below we present an excerpt of a typical SIP message along with the included SDP headers and the information that needs to be preserved for further analysis. The forensically interesting data are shown in bold font.

```
Time 2013-05-01 23:35:57.978170
Internet Protocol Version 4, Src: 5.xx.xx.210 (5.xx.xx.210), Dst: 192.xxx.xxx.37 (192.xxx.xxx.37)
Session Initiation Protocol
Request-Line: INVITE sip:71150@sip.xxxx.gr SIP/2.0
Message Header
Via: SIP/2.0/UDP 5.xx.xx.210:61624;branch=z9hG4bK-d8754z-320fc157e67ba641-1---d8754z-;rport
Contact: <sip:402@5.xx.xx.210:61624>
To: "71150"<sip:71150@sip.xxxx.gr>
From: "jpsaroud windows"<sip:402@sip.xxxx.gr>;tag=3f498445
Call-ID: MmFmYWFjNTk1ZTQzOTdhM2JiODJiNDAYZGNkOTRiZmU.
CSeq: 1 INVITE
User-Agent: eyeBeam release 1102q stamp 51814
Session Description Protocol
Owner/Creator, Session Id (o): - 5 2 IN IP4 5.xx.xx.210
Owner Network Type: IN
Owner Address Type: IP4
Owner Address: 5.xx.xx.210
Session Name (s): CounterPath eyeBeam 1.5
Connection Information (c): IN IP4 5.xx.xx.210
Connection Network Type: IN
Connection Address Type: IP4
Connection Address: 5.54.64.210
Media Attribute (a): alt:1 4 : UhYE2Wox sLbn3kLo 5.54.64.210 24784
Media Attribute (a): alt:2 3 : R828U4V/1W4gLyQM 10.10.10.1 24784
Media Attribute (a): alt:3 2 : M4f701Fm 5Gw9wOoX 192.168.61.1 24784
Media Attribute (a): alt:4 1 : BndXE2LR CPxnI5x9 192.168.111.1 24784
Info: Request: INVITE sip:71150@sip.xxxx.gr, with session description
```

3.2.2 OPTIONS Request

OPTIONS request is a keep-alive mechanism to assist in determining whether a remote user agent/SIP server is presently available before actually placing a phone call. It is also used to enable a SIP entity to query for the capabilities (such as audio codecs available for the RTP stream, available extensions of a remote SIP entity, etc.) in advance of establishing a dialog without "ringing" the remote entity (RFC3261).

From a forensics perspective it appears that malicious users make use of this attribute in order to perform a reconnaissance task and discover available SIP servers in a given network. Similar to a ping scan used for revealing alive hosts, an OPTIONS scan can expose alive SIP servers and their programmed extensions. Furthermore, if OPTIONS messages are used for fingerprinting a network they are not normally detected as an attack by an IDS (snort in OSSIM was tested) and are not logged from SIP servers (Asterisk servers tested). This is because OPTIONS is not malicious in its nature and purpose, but this mechanism is open to abuse by an attacker. As such, this type of attack remains invisible to the network administrator but can be disclosed by the proposed application.

3.3 SIP Response Codes

3.3.1 STATUS 200 OK with session description

As mentioned earlier a "Status 200 OK" response message is sent to a remote host after a successful SIP INVITE or REGISTER request.

From a forensics perspective it was also observed that some applications report their private IP address during an OPTIONS reply message to their respective registration server. Remote SIP User Agents reply to an OPTIONS request with a "*STATUS: 200 OK*" message with session description (SDP). The private IP address is found inside the SDP Owner and the SDP Connection Info headers.

3.3.2 4xx—Client Failure Responses

Indication of malicious activity is considered when the SIP server responds to repetitive unsuccessful SIP INVITE messages, that is, “404 Not Found”. When the server is programmed to accept anonymous requests, a 404 message is an indication of a reconnaissance scan. If the server accepts anonymous requests, then an IDS rule can be in force that accumulates the number of unsuccessful requests from a single IP and alerts if a set threshold of number of failed requests is exceeded. However only the server maintains the information of valid SIP extensions (Dial Plan) and can distinguish between a 404 relating to a valid yet unavailable and a 404 caused by a non-existent extension (Fig.3).

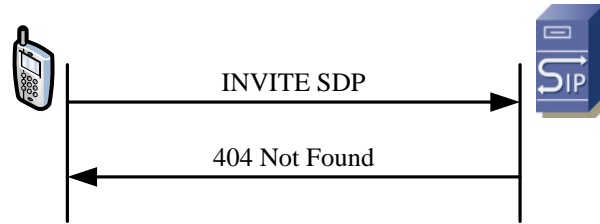


Figure 3: Unsuccessful SIP INVITE negotiations

On the other hand when a SIP Server is configured to allow only authenticated users, a SIP response like "Status 403 Forbidden"/"Status 401 Unauthorized" is sent. Repetitive alike messages are a strong indication of an on-going brute force attack.

3.4 Malicious Activity Detection Process

Through a data mining process in the formed artifact database we are able to discover some indications or even proof of malicious activity. Before we proceed to describing the detection process we first define a series of relevant terms and set a list of assumptions as follows:

Internal Users. We define as internal users those who have an account in one of the SIP servers of the organization. The accounts that have been created and used for this project is assumed that during the baseline phase are not compromised. Any new account that is created goes through a baseline phase. An internal user can access the SIP services from either inside or outside the organizations' data network premises. A user may place a call with another user of the same SIP server or with a user that is registered to a different SIP server.

External Users. We define as external users those who do not have a valid account to any of the SIP servers of the organization. An external user may place a call for an internal user and vice versa.

Baseline phase. We define as a baseline phase for the internal users a period of time of normal user activity. We consider as normal activity the installation of the provided account into only one device (PC softphone, mobile device softphone, IP phone, Analog Phone adapter) with ordinary daily usage. During this phase we assume or reinsure no malicious activity or compromise. This is similar to building a profile for anomaly detection IDS type of approaches (Katos, 2005).

Internal User profile. We define as a user profile a set of attributes that their values remain constant during the baseline phase. These attributes are derived from the information contained in the SIP headers (Table 1) as well as from the underlying business logic that is reflected by the users' "trends" and behavior. Especially in SDP Media Attributes header, where we have a lot of information we can store a MD5 hash value in order to do the comparison. In this work we constructed three internal users' profiles, as described below.

Fixed. By the term *Fixed* we denote the user profile that matches the operation of VoIP adapters, IP phones and VoIP capable routers (usually with a FXS interface). The main characteristics of this profile are the absence of changes in a series of attributes such as the IP (either Public or Private) and a 24 hours daily operation of precise interval registration.

PC Softphone. This refers to a different user profile, where we include the PCs that run a VoIP software application. The main characteristics of this profile are the regular and benign changes of IP address typically reflecting roaming scenarios or IP changes due to DHCP operations.

Mobile. This is also a user profile. In this profile we include the mobile devices (smartphones, tablets) that run a VoIP software application with a HSPA or Wi-Fi connection to the Internet. The main characteristics are the frequent changes of the public IP address and a daily hour's operation.

3.4.1 GeoIP information

In a typical organizational setting, SIP is allocated to users who may have a given geographical distribution and the access policy can be configured to reflect such distribution. During our empirical evaluation we were able to verify this assertion.

All users who participated in this research were found to be located in Greece and Belgium as expected. We used the Maxmind database (Maxmind Geolite, June 2013) and we did confirm the accuracy of the GeoIP results in the base of the Country.

We summarize the profile attributes in Table 2.

Attribute		Fixed	PC Softphones	Mobile	
1.	User Agent	Operating System	Constant (firmware)	Constant	
2.		Application Name	Constant	Constant	
3.		Device	Constant	N/A	Constant
4.	Private IP		Constant	Variable	Variable
5.	Caller ID		Constant	Constant	Constant
6.	Source IP		Applicable to User	Variable	Variable
7.	GeoIP (Source IP)		Constant (City)	Constant (Country)	Constant (Country)
8.	SDP Media Attributes		Constant (Specific to User Agent capabilities and User Preferences)	Constant (Specific to User Agent capabilities and User Preferences)	Constant (Specific to User Agent capabilities and User Preferences)s
9.	Register intervals		Constant	Constant	Constant
10.	Daily Routine (trend)		Constant	Specific to User	N/A
11.	401 messages		Constant	Constant	Constant
Total of constant values		10	7	8	

Table 2 : Baseline User Profiles Table

We also consider that both internal and external users may behave in a malicious manner. For example an internal malicious user may place a threatening call and then deny it. He may claim that his account was compromised. In addition the fact that he is behind a NAT server makes him believe that he is undetectable.

An external user may try to take advantage of a SIP server's misconfiguration that will allow him to place a free call or even may try to brute force a valid account.

3.4.1.1 Malicious Activity Detection of Internal Users

Malicious Activity Detection of Internal Users is detected through statistical analysis. Every internal user is assigned with a profile according to his type of device and use. When the baseline phase is complete we can fill in Table 2 with the derived constant values. Periodical checks in the artifacts database can monitor any change in the profile's constant values. Every change in these attributes must be investigated against a possible attack.

3.4.1.2 External users

In order to detect malicious activity from external users we use a different approach. More analytically, we constructed the following list of series of events and actions that are needed to run and be checked periodically:

- OPTIONS method scans. As already mentioned, we consider repetitive OPTIONS requests from a single IP as a part of a reconnaissance phase of an upcoming attack aiming to identify available SIP servers in a network. Any OPTIONS scans incident needs to be investigated.
- 401 and 404 messages to external IPs. As stated before, repetitive 401 and 404 response messages are sent to a specific IP address who issues INVITE or REGISTER requests.

- Spoofed Headers. We noticed that the SIP server’s logging is based on the SIP headers that are easy to be spoofed. We check for spoofed data in various headers for a given source IP. More precisely we check in the SIP From header, the SDP Connection Info, and the User Agent for spoofed data.
- User-agent. We check the value of the User-Agent against a list of known user-agents.
- Empty SDP. An INVITE request should contain the SDP connection info. INVITE messages with empty SDP information is an indication that the caller’s primary goal is not to actually place a call.
- Private IP. Whenever possible, we record the private IP of the external user. Although not useful during the detection process, it may really be helpful when an investigation is underway for identifying the real attacker.

3.4.2 Correlation Process

The findings and normalized data from the previous steps will also go through a correlation process and will be combined with information from various sources. Firstly we need to examine the root cause of the 404 messages. The process attempts to identify whether these messages are provoked due to unavailable users or because of a free call attack. This is achieved by correlating the calling number with the servers’ dial plan. OPTIONS scans are correlated against the list of operating SIP servers and GeoIP information. Spoofed headers and User-Agent values are correlated with information from an IDS with well defined signatures. The same correlation process is also followed for internal users if they are found to cause 4xx messages.

4 Evaluation

The implementation of the proposed framework involved the development of a number of tools and scripts. The network captures were performed with the tcpdump utility. The parser leveraged utilities such as the *tshark* software which is the command line tool of the wireshark network analyzer application, *sed* and *awk*. The database that was employed is MySQL. Database views were used to manage the data retrieval complexity and improve data access speed. For instance, several views were built with mappings of date time, username, user-agent, remote public IP and remote private IP. Furthermore views were setup aiming to identify ongoing attacks with repetitive failed “REGISTER” and “INVITE” requests while views with repetitive “OPTIONS” requests were used to highlight reconnaissance activities of an upcoming attack. Needless to mention, the application is also capable of preserving evidence such as remote IPs and fake or spoofed User-Agent information.

In order to evaluate the framework, a network traffic capture of the University’s border router connection to the Internet was set up (Fig. 5). The University’s border router has a Gigabit Ethernet connection and advertises nine class C networks through Border Gateway Protocol (BGP). The traffic capture was performed over a period of ten days.

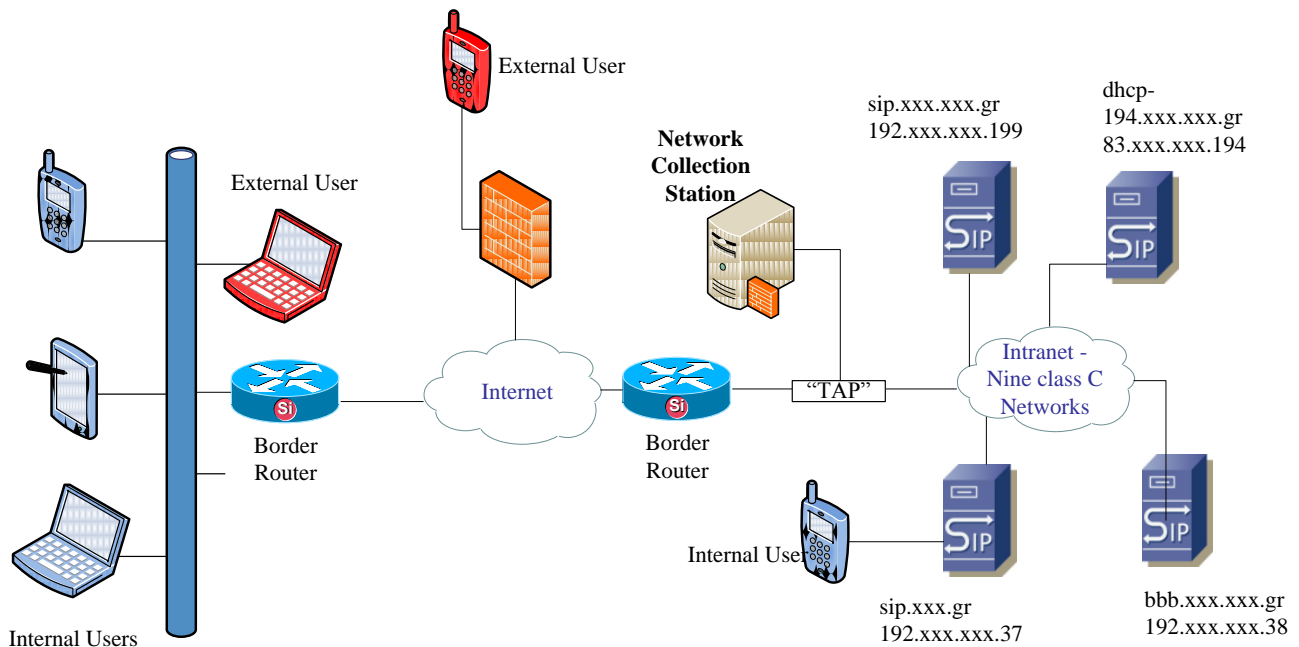


Figure 4: Network traffic capture layout

From a technical perspective, the acquisition is feasible by employing a gigabit Ethernet switch capable of mirroring all available virtual LAN (VLAN) ports to a specific port (tap). The tap fed the collected data to the network collection station. It is a host that after acquiring the SIP data (normally creating a pcap file), it parses them, extracts the relevant headers (described in Table 1) and stores them in a database. In production environments the network monitoring station should also be equipped with a second network interface connected to the management VLAN allowing remote connections.

Upon collection, normalizing and storage of the SIP data, the analysis component (database views) will extract the values for each internal user. It will then fill in its corresponding user profile. It will then search for indications of malicious activity according to the proposed methods. The findings will be correlated with the information provided by the underlying policies (such as dial plans) and from other sources (such as GeoIP information, OSSIM IDS) in order to pin down the malicious attempts against the SIP infrastructure.

4.1.1 Internal users' profiles filling

We created 16 sip accounts on 3 different SIP servers and delivered them to a group of users who were located in Greece and Belgium. The accounts were installed in 16 different devices including IP phones, one router with VoIP capabilities and PCs and smartphones with software phones. During the baseline phase we were able to populate the database by filling in the information described in Table 3 for each user. For brevity reasons we present the findings for 5 of them which cover all the cases. It is worth mentioning that all 5 devices were outside University premises connected though another ISP.

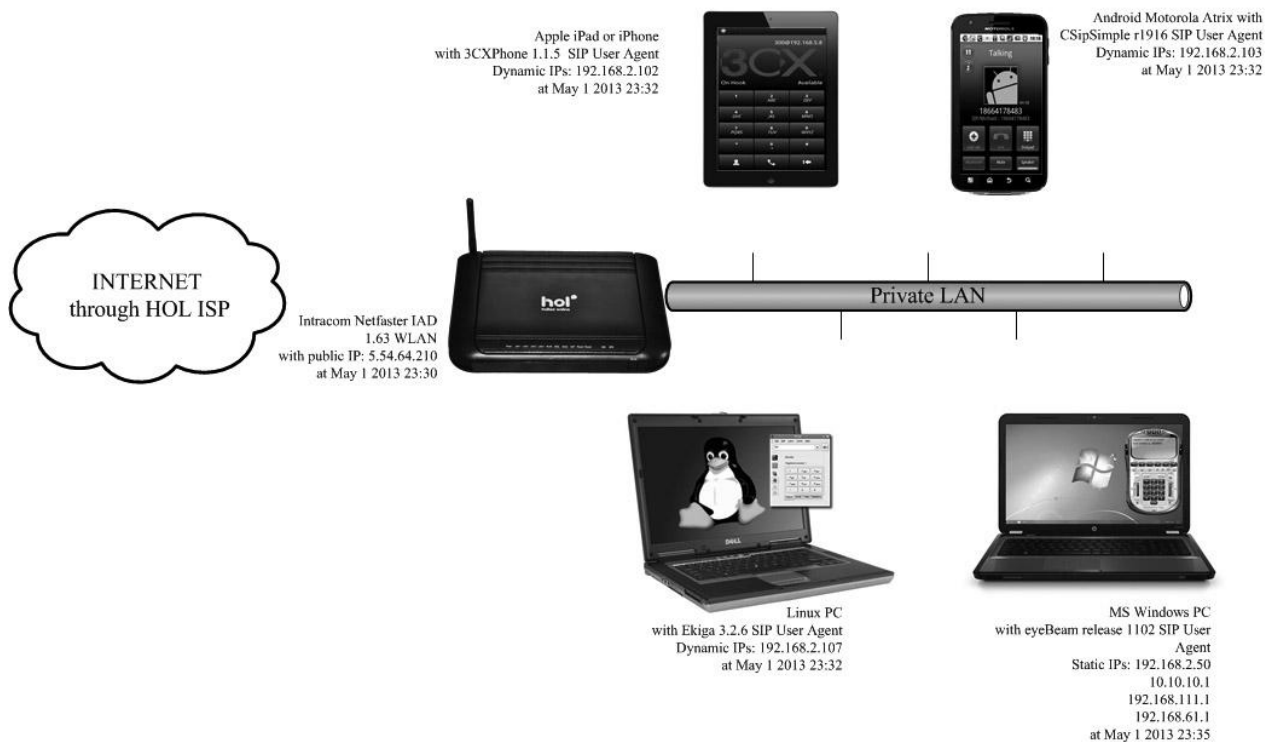


Figure 5

		Attribute	Fixed	PC Softphones	PC Softphones	Mobile	Mobile
1.	User Agent	Operating System	1.63 WLAN	Linux	MS Windows	IOS	Android
2.		Applications Name	N/A	Ekiga 3.2.6	eyebeam r1102	3CX 1.1.5	CSipSimple r1916
3.		Device	Intracom	N/A	N/A	Apple Ipad or	Motorola

		Netfaster IAD			IPhone	Atrix
4.	Private IP	Constant	Variable	Variable	Variable	Variable
5.	Caller ID	404@sip.xxx.gr	403@sip.xxx.gr	jpsaroud home 402@sip.xxx.gr	603@sip.xxx.x xx.gr	604@sip.xx x.xxx.gr
6.	Source IP	5.xx.64.210	Variable (5.xx.64.210)	Variable (5.xx.64.210)	Variable (5.xx.64.210)	Variable (5.xx.64.210)
7.	GeoIP (Source IP)	Greece	Greece	Greece	Greece	Greece
8.	SDP Media Attributes	Omitted for brevity	Omitted for brevity	Omitted for brevity	Omitted for brevity	Omitted for brevity
9.	Register intervals	45 min	60 min	55min	50 min	15 min
10.	Daily Routine (trend)	Day/Night	Afternoon	Afternoon	Daylight	Daylight
11.	401 messages	"No"	"No"	"No"	"No"	"No"
	Total of constant values	10		7		8

Table 3: Internal Users filled profiles

None of the legitimate users changed the profile's constant values except for one user in Belgium who travelled to Luxembourg and the USA and this information was reflected in his profile. The incident was investigated and it was revealed that the Luxembourg case was because of a roaming Wi-Fi. The USA location was reported because the underlying application (Acrobats) was using a server in the USA as a rendezvous point when IOS was in sleep mode.

4.1.2 External User Malicious Activity Detection

After applying the method for the external users and examining the event list described earlier in this paper, we obtained the following results (Fig. 6). Unsuccessful REGISTER attempts were about 77% of the total attacks. It is obvious that the attacker believes that gaining access to an account will grant him with cost free calls. The malicious users tried to register to one of the monitored SIP servers by testing various possible accounts. It appears that the goal was not to brute force one specific account by a dictionary attack. Instead they tested a huge combination of possible user accounts with no password set. This can be crosschecked with the information provided by the dial plan. A large group of nonexistent users verifies the attack. GeoIP information is yet another factor to confirm the attack.

Unsuccessful INVITE requests were about 19% of the total attacks. It appears that the malicious users tried to place a call without prior exploitation of a valid account. This can be observed in the case of a misconfigured SIP server for example. As an INVITE request is a legitimate one, it cannot be tracked by an IDS. In order to verify that an unsuccessful INVITE is actually a malicious one, we crosscheck the callee with the information provided by the dial plan. In such case, a nonexistent callee can confirm the attack. Moreover it was discovered that attackers sometimes tried to exploit server vulnerabilities by using special characters in the dialed string. GeoIP information is another source of information to confirm the attack.

OPTIONS requests account to the 4% of the total attacks. OPTIONS requests were used in order to identify SIP running servers in the network. Correlation with known SIP servers inside the organization and the GeoIP information of the remote user confirms the malicious intention of the OPTIONS request.

It appears that popular VoIP auditing tools have been transformed to attack tools. We were able to identify two of them, namely the SIPVicious and the Sip/Cli auditing tools. SIPVicious is a popular open source software suite to audit VoIP capable PBXs based on the SIP protocol, written in Python (SIPVicious, 2013). A number of variants of SIPVicious are available aiming to change the signatures of software (such as the crucial User Agent value) in order to avoid detection from IDS software. It appears that SipVicious was used in the vast the majority of the attacks as it supports the INVITE, the REGISTER and the OPTIONS requests methods (Fig. 7).

SipCli is a command line SIP user agent that runs on Microsoft Windows operating systems (SipCli, 2013). It is designed for penetration testing of VoIP software PBXs. It sends SIP INVITE messages with the option to set source IP interface, SIP port, SIP proxy/port, SIP username and password. During our tests it was mainly used as a brute-force attack tool.

The most common attributes is the name of the User-Agent used that is "sipcli/v1.8" and the presence of SIP body text with SDP headers. The latter reveals the private IP address of the attacker if located behind a NAT server.

We discovered another attacking tool which was used occasionally. We weren't able to identify the application. However its main characteristic was that it spoofed almost every possible field.

A thorough analysis of the findings related to the malicious users and their attacking tools can be found in our supporting website [blinded for review].

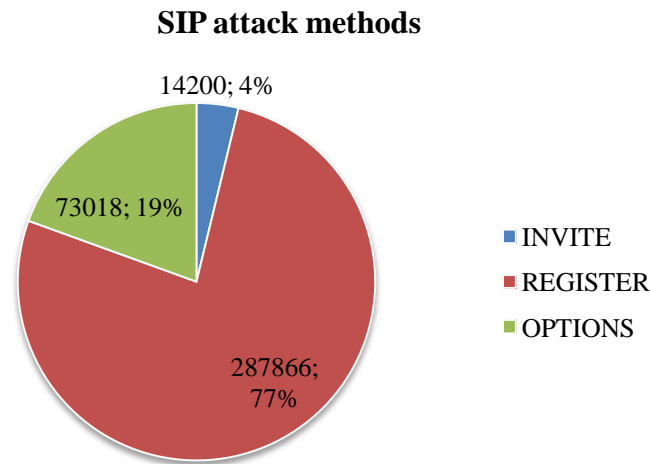


Figure 6: SIP request methods used in identified attacks

Many of the above attacks were also identified by the operational IDS. The signature tried to match the value “friendly-scanner” of the SIP User Agent of the SipVicious tool. However we discovered variants of the SipVicious as its source code is freely available on the Internet. It is very easy for anyone to change the value of the User Agent header.

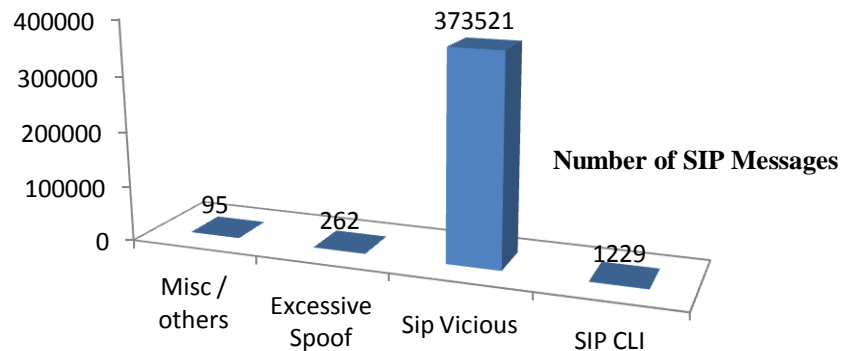


Figure 7: Tools identified during the SIP attacks

4.1.3 Troubleshooting

A side benefit of the application is that it can provide to the administrator activities for exposing various service errors. For instance, the number of SIP messages received from a valid internal User Agent over time indicates network activity and can be used to deduce conclusions on the health state of the network. As such, an excessive amount of SIP messages can be an indication of a network appliance misconfiguration and the network administrator must be alerted. Error messages from SIP Servers with error codes such as "500 Internal Server Error" can also guide the system administrators to detect and correct such errors in a timely manner.

4.1.4 Comparisons with existing logging methods

If we do a comparison of the proposed scheme for collecting and preserving SIP artifacts and traditional server logging, we can draw up some conclusions that are presented in Table 4.

Artifact	Proposed Scheme Logging	Server Side (asterisk) Logging
User agent		
Operating System	Yes	No
Application	Yes	No
Device	Yes	No
Private IP	Yes	No
Source IP (REGISTER)	Yes	Yes
Source IP (INVITE)	Yes	No (SIP channel only)
Unauthorized 401	Yes	Yes
Not Found 404	Yes	Yes (Indirect)
SIP From (Caller ID)	Yes	Yes
OPTIONS method	Yes	No
Encrypted data	No	Yes

Table 4 : Comparison between Network logging and Server logging

We can also derive some benefits of the proposed logging scheme.

1. Vendor / Platform independent
2. Create logs even for devices that are incapable of producing enriched logs (aka VoIP adapters, mobile softphones)
3. Normalized logs, easy process and correlation with other sources.

The proposed method is agnostic of the current SIP infrastructure of an organization. This approach is easy to deploy and it is independent of the vendor or platform of the existing servers. The only prerequisite is compliance with the SIP protocol. However, we expect that this approach can be adapted to operate in other VoIP standards.

This solution provides us also with the ability to produce logs for every SIP capable device. During the experiments and the development of the application we came across persistent attacks targeting stand alone SIP devices. Even if we enabled syslog messages on an IP phone, the provided logging information is insufficient as the forensically interesting traffic data are not included in a standard log. In addition there are applications with no logging capabilities at all such as softphones on mobile devices. Finally, the produced logs are already normalized and they can be easily processed and correlated with information from other sources.

4.1.5 Similarities and Differences between IDS and Network logging

We can point out some differences between an IDS and the proposed network logging. They both perform deep packet inspection but also exhibit key differences. For an IDS, if a packet matches a rule, it will be logged and an alarm will be triggered. An IDS also performs real time inspection, making it a monitoring tool. For the network logging approach all packets are systematically logged and alerts are generated during the audit stage. As such, network logging is not designed to operate as a real time detection process, although capturing is performed in real time. In addition, network logging will require a significant amount of storage.

Against the above it can be concluded that the proposed method is not a solution that comes to replace existing server logging or an IDS. It is a complementary tool to support forensic readiness. The main goal is to gather volatile SIP artifacts that can be used during an investigation of an incident and to increase the reliability of the IDS.

5 Legislation limitations on operating this application on a network

In this section we develop some concerns on implementing this solution in production networks. Proactive creation and preservation of evidence facilitate without any doubt the investigation in a successful and cost-effective manner. Forensic readiness is proved to be valuable when – especially - volatile data have to be acquired and preserved. However, needless to say, the process of a forensic investigation is subject to considerable scrutiny of both the *integrity of the evidence*, meant as the “information by which facts tend to be proved”, and *the integrity of the investigation process* (Rowlingson 2004). When developing such an approach we should take into consideration that it raises ethical and legal issues pertaining to the secrecy of communications and privacy of the concerned persons and that the lawfulness and, consequently, the admissibility of evidence in court depend upon the respect of legal constraints and guarantees, laid down in legislation pertaining to communicational and informational privacy.

Firstly, (massive or routine) proactive collection and preservation of evidence as such undermines the “traditional” current constitutional model, which relies upon gathering conclusive evidence of wrongdoing of suspect individuals. A model that equates forensic readiness with indiscriminate collection of probably useful evidence that is carried out against individuals at random would blow up the cornerstones of the rule of law state (Hoffmann-Riem, 2002), as it would perceive all citizens as potentially future threats (Lepsius, 2004) if not offenders and criminals. Extended production and collection of evidence mirrors the shift from a constitutional state guarding against the threat of specific risks in specific situations toward a security-orientated preventive state, which acts operatively and proactively but at the same time interferes with the fundamental rights and freedoms of the citizens (Mitrou 2008).

Traditionally, the interception and collection of content data (i.e., the meaning or purport of the communication, or the message or information being conveyed by the communication) has been a useful tool for law enforcement authorities. When introducing evidence collection approaches into an infrastructure we should bear in mind that - even if content the communication is not intercepted - evidence gathering and readiness is based upon the collection and logging of the so-called subscriber’s and/or communication/traffic data. The use of such a method for law enforcement purposes (or even for the purposes of corporate forensics) is subject to the conditions and procedures provided by the respective law pertaining to the protection of communications secrecy and informational privacy.

The provisions of the EU e-Privacy Directive relate to “traffic data” as “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof” (Art. 2 b). Different communications infrastructures give rise to different forms of transactional data (Rotenberg et. al 2006). The e-Privacy Directive covers all traffic data “in a technology neutral way,” i.e. those of traditional circuit-switched telephony as well as packet-switched Internet transmission. The Convention of the Council of Europe on Cybercrime (2001), assigning “traffic data” to a specific legal regime, defines it as “any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication’s origin, destination, route, time, date, size, duration, or type of underlying service” (Art. 1 d). Under European Law (Data Protection Framework Directive), to the extent that this data is relating to an identified or identifiable natural person, it is deemed to be “personal data” (Art. 2 a). In United States law (Stored Communications Act), “transactional” data lists certain customer record information: the customers’ name, address, phone numbers, billing records, and types of services the customer utilizes. The USA PATRIOT Act (2001) expanded this list to include “records of session times and durations,” any temporarily assigned network address, and “any credit card or bank account number” used for payment (Mitrou 2008).

Highly important for law enforcement purposes are the measures of traffic data preservation and data retention. As underlined in the Explanatory Report of the Cybercrime Convention of the Council of Europe, traffic data might last only ephemerally, which would make it necessary to order its expeditious preservation. In the language of the Cybercrime Convention, data preservation is the procedure of keeping stored data secure and safe. The preservation measures apply also to computer data that “has been stored by means of a computer system,” which presupposes that the data already exists, has already been collected, and is stored. Expedited data preservation claims, within the framework of a specific investigation or proceeding, the right for the relevant authorities to compel a provider (already in possession of certain data on a specific subscriber/user) to conserve it against the possibility of disappearing. *The Convention sets out procedural powers to be adopted by the signing states: expedited preservation of stored data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of computer data; realtime collection of traffic data.*

According to the European Convention on Human Rights communications surveillance is unacceptable, unless it fulfills three fundamental criteria set in Art. 8 (2): (1) a legal basis, (2) the need/necessity of the measure in a democratic society, and (3) the conformity of the measure with the legitimate interests of national security, public safety, or the economic well-being of a country, prevention or disorder of crime, protection of health or morals, or protection of the rights and freedoms of the others (Coemans and Dumortier 2003). As specified by the European Court of Human Rights in the case *Copland v. United Kingdom*, the creation, retention and/or preservation of traffic data falls under the protection of communicational secrecy, which means that the need for - especially proactive - evidence gathering and storing has to be weighed against the harms and infringements for communicational privacy. The objective pursued must be balanced against the seriousness of the interference, which is to be judged taking into account, inter alia, the number and nature of persons affected and the intensiveness of the negative effects. For these reasons such a method should be implemented only in relation to crimes that are regarded by the law as “severe” or “national security threats” and with specific institutional conditions to be fulfilled in order to investigate a criminal incident in accordance with necessity and proportionality requirements.

6 Conclusions and future work

In this paper we examined the feasibility of conducting forensic investigations in VoIP infrastructures and presented a framework for collecting and analyzing the data that can potentially detect attacks and reveal information including private IPs, network topologies and end user equipment. The popular SIP protocol was used as a vehicle to demonstrate the processes for correlating and interpreting the forensic artifacts. An advantage of the proposed framework over existing approaches like

DEFSOP presented in the beginning of this paper is that all the data required for extracting the necessary evidence can be directly obtained by the (local) network captures without the requirement of a special data collecting agent installed on the SIP entities.

The importance of forensic readiness is evident, as it is realized that if certain volatile network data are not captured, recorded and logged (which is the case in most VoIP deployments), it would not be possible to identify and trace an attack to its origin. Since VoIP is becoming a very popular technology adopted by a large number of users worldwide, it is imperative for the SIP provider to cater for forensic readiness capabilities as it is expected that the attacks will be frequent, affect many legitimate users and may cause a financial damage to both operators and end users. The tools used for attacking VoIP services are widely available. In fact, most of them have existed for a while now as they were initially developed for serving security audit purposes.

Furthermore, the benefit of promoting forensic readiness practices is twofold. First, it supports the identification of the source of a threat and an attacker as mentioned earlier. Second, it provides invaluable information and feedback to the administrators for debugging purposes and for facilitating troubleshooting when required.

It was also shown that the additional layer of complexity introduced in an internetworked environment by using VoIP solutions has a negative impact on privacy. Therefore the tradeoff between privacy and accountability needs to be carefully addressed with both technical and legislative controls.

Future work involves the further development of the tools and its integration with IDSs in order to support real time operation. In addition, the framework will need to be enriched with applications capable of performing similar analysis on VoIP technologies other than SIP, such as H.323 and possibly closed systems such as Skype.

6.1 References

1. Coemans, C. and Dumortier, J., Enforcement issues—Mandatory retention of traffic data in the EU: Possible impact on privacy and on-line anonymity, in *Digital Anonymity and the Law*, Nicoll, C. Prince J.E.J., and van Dellen, J.M., Eds., TMC Asser Press, The Hague, the Netherlands, 2003, 161.
2. Davidoff S., J. H., *Network Forensics: Tracking Hackers through Cyberspace*. Prentice Hall, 2012.
3. Dwivedi, H, *Hacking VoIP Protocols, Attacks, and Countermeasures*. No Starch Press, 2009.
4. François, J.; State, R.; Engel, T.; Festor, O., "Digital forensics in VoIP networks," *Information Forensics and Security (WIFS)*, 2010 IEEE International Workshop on , vol., no., pp.1,6, 12-15 Dec. 2010
5. Gritzalis D., Katos V., Katsaros P., Soupionis Y., Psaroudakis J., Mentis A., "The Sphinx enigma in critical VoIP infrastructures: Human or botnet?", in *Proc. of the 4th International Conference on Information, Intelligence, Systems and Applications (IISA-2013)*, IEEE Press, Greece, July 2013.
6. Handley M., Jacobson V., Perkins C. SDP: Session Description Protocol, RFC 4566, <http://tools.ietf.org/html/rfc4566>, 2006
7. Hoffmann-Riem, W., Freiheit und Sicherheit im Angesicht terroristischer Anschläge, *Zeitschrift für Rechtspolitik*, 35, 2002, pp 497-505
8. Hsien-Ming Hsu, Yeali S. Sun, Meng Chang Chen, Collaborative scheme for VoIP traceback, *Digital Investigation*, Volume 7, Issues 3–4, April 2011, Pages 185-195, ISSN 1742-2876
9. I-Long Lin, Yun-Sheng Yen, "VoIP Digital Evidence Forensics Standard Operating Procedure", *International Journal of Research and Reviews in Computer Science(IJRRCS)*, Vol 2, No 1 (2011).
10. Infonetics Research. \$377 billion to be spent on VoIP and UC services over next 5 years. <http://www.infonetics.com/pr/2012/VoIP-UC-Services-Market-Highlights.asp>, Accessed on 05.06.2013
11. Irwin David, Slay Jill, " Extracting Evidence Related to VoIP Calls", G. Peterson and S. Shenoj (Eds.): *Advances in Digital Forensics VII*, IFIP AICT 361, pp. 221–228, 2011.
12. Katos Vasilios,"Network Intrusion Detection: Evaluating Cluster, Discriminant, and Logit analysis". *Information Sciences*, vol. 177, No.15, pp. 3060-3073, 2007

13. Keromytis Angelos D. Voice over IP security: research and practice. IEEE Security and Privacy March 2010.
14. Lepsius, O., Liberty, security and terrorism: The legal position in Germany, Part 2, *German Law Journal*, 5, 2004. pp. 435-460
15. Maxmind GeolIP database, <http://dev.maxmind.com/geoip/legacy/geolite>, Accessed on June 2013
16. Mitrou L., Data Retention: a Pandora Box for Rights and Liberties?, in A. Acquisti/S. De Capitani di Vimercati/S. Gritzalis/C. Lambrinouidakis (Eds.), *Digital Privacy: Theory, Technologies and Practices*, Auerbach Publications, 2008, pp. 410-433.
17. Psaroudakis I., Katos V., Efraimidis P. A framework for anonymizing GSM calls over a smartphone VoIP network. Proc. of the 27th IFIP International Information Security and Privacy Conference, Springer IFIP AICT, Greece, June 2012, pp. 543-548.
18. Rosenberg, J., Schulzrinne, H., Camarillo, G. SIP: Session Initiation Protocol. RFC3261, June 2002.
19. Rotenberg, M. Privacy and human rights 2005—An international survey of privacy laws and developments, Electronic Privacy Information Center, Privacy International, <http://www.privacyinternational.org/index/> September 7, 2006.
20. Rowlingson, R., "A ten Step Process for Forensic Readiness", *International Journal of Digital Evidence*, Winter 2004, Volume 2, Issue 3. Available at: <http://www.utica.edu/academic/institutes/ecii/ijde/>
21. Simon M, Slay J. Voice over IP: forensic computing implications. In: 4th Australian digital forensics conference; December 2006.
22. SipCli VoIP audit tool, <http://www.yasinkaplan.com/SipCli/>,. Accessed on 13.06.2013
23. Sipvicious VoIP audit suite. <http://blog.sipvicious.org/>. Accessed on 13.06.2013
24. Walsh, T.J.; Kuhn, R., "Challenges in securing voice over IP," *Security & Privacy, IEEE* , vol.3, no.3, pp.44,49, May-June 2005
25. Yun-Sheng Yen, I.-Long Lin, Bo-Lin Wu, A study on the forensic mechanisms of VoIP attacks: Analysis and digital evidence, *Digital Investigation*, Volume 8, Issue 1, July 2011, Pages 56-67, ISSN 1742-2876

6.2 APPENDIX A

The geolocation identification of the malicious users (Fig. 8). An up to date distribution of attacks is maintained in http://isir.ee.duth.gr/?page_id=267. For every mark there is detailed information about the type of the attack along with the tool used. Colour indicates the tool used. User agent information is maintained for internal users (Fig. 9).

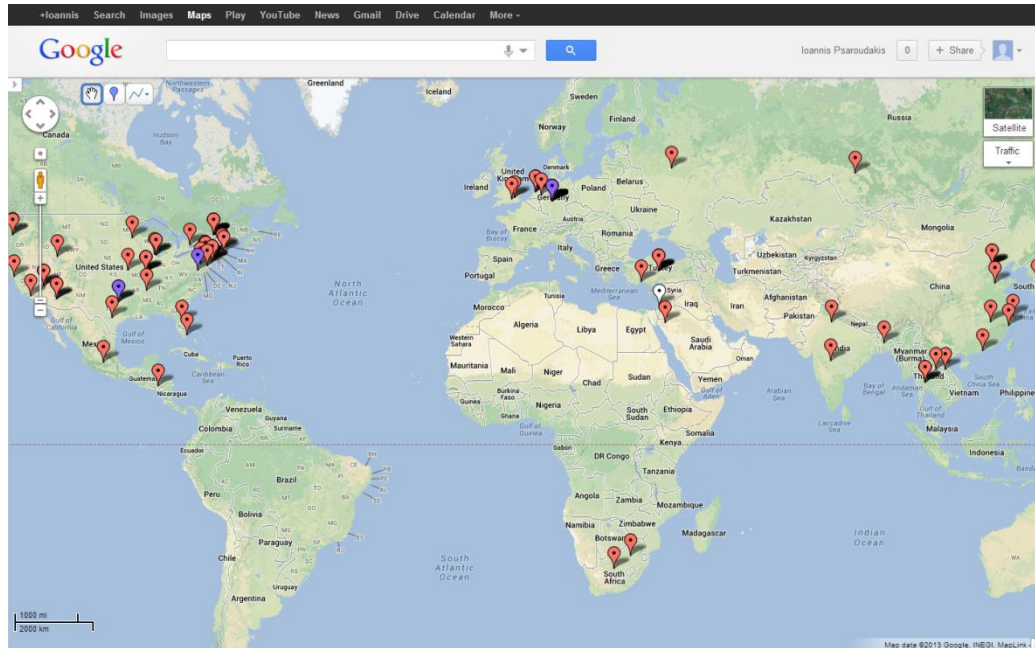


Figure 8: malicious users' GeoIP

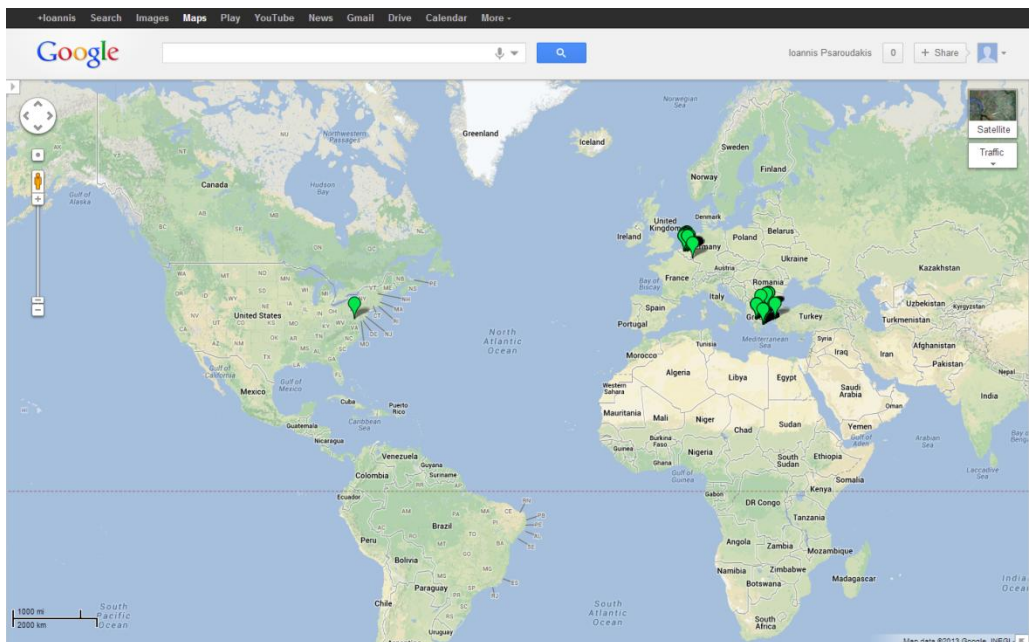


Figure 9: GeoIP location of Internal Users