A Review on Detecting an Attackers in VOIP using Honeypot

Kurhade Supriya B.[1] Palwe Chaitali B.[2] Pande Priyanka R.[3]
[1,2,3]Department of Computer Engineering
[1,2,3]JCOE, Kuran

Abstract—The number of users of VoIP services is increasing every year. Basically, VoIP systems are more attractive for attackers. This paper describes the implementation of a low interaction honeypot for monitoring illegal activities in VoIP environments. The honeypot operated during 92 days and collected 3502 events related to the SIP protocol. The analysis of the results allows understanding the modus operandi of the attacks targeted to VoIP infrastructures. These results may be used to improve defence mechanisms like firewalls and intrusion detection systems. SIP is one of the major VoIP protocols and has its architecture composed of four basic elements: user agent, SIP proxy, redirect server and registry server. The user agent (UA) is a logical function that matches the architecture of the client. It is responsible for initiating or replying to SIP transactions and can act as both client (UAC) and as a server (UAS), starting SIP requests and SIP responses accepting, or accepting SIP requests and answering them, respectively. There are few implementations on VoIP security and attacks in real-world VoIP systems. Some of them propose the use of honeypots to catch malicious traffic in a VoIP environment. Honeypots can be defined as a computational resource to be probed, attacked and / or compromised, whose value lies precisely in the unauthorized or illegal use of the resources offered.

Key words: VOIP, Honeypot

I. INTRODUCTION

Currently the telecommunications universe is undergoing a transformation, with migration increasingly constant voice communication via circuits switched to voice communication via IP network, also known as VoIP. This migration provides users a variety of new services and facilities. In the case of VoIP communications one of the main difficulties are related to security, with new attacks aimed at compromising a production environment. A system that suffered before, mostly with attack on physical infrastructure, will now take all threats directed to the protocol stack TCP / IP Come too specific attacks targeted at voice protocols such as SIP (Session Initiation Protocol), IAX (Intra-Asterisk Exchange) and RTP (Real-time Transport Protocol), among others.

SIP is one of the major VoIP protocols and has its architecture composed of four basic elements: user agent, SIP proxy, redirect server and registry server. The user agent or user agent (UA) is a logical function that matches the architecture of the client. Responsible for initiating or replying to SIP transactions, can act as both client (UAC) and as a server (UAS), starting SIP requests and SIP responses accepting, or accepting SIP requests and answering them, respectively.

Responsible for routing function in a SIP network, the SIP proxy is intended route the SIP requests and responses between the devices involved, for the purpose of completing calls from UAC. The redirect server aims to redirect requests and responses based on SIP messages from class 300, directing the UAC to direct contact to the requested destination. But the registration server is responsible for registering information on any UA that has already logged on to the system. As well as the development of other security component technology was not developed with the same efficiency and speed dedicated to the delivery of applications and the provision of the service. Consequently a variety of attacks on these systems have emerged (e.g. Call tracking, information leakage, call handling, injection control codes). Despite having some knowledge of these attacks, it is not possible to gather consistent and reliable information about the method, tools and motivations that lead attackers to execute them.

II. VOIP SECURITY

Threats to VoIP environments security comprise the whole of the problems faced by data networks, more specific problems of integrated protocols and services to a VoIP infrastructure [7]. With respect to threats intended for environments with VoIP infrastructure, there are various ways to categorize them. A possible taxonomy is given in [2] and classifies the attacks as threats to the availability, confidentiality, integrity and against the social context.

A. Threats against Availability:

Threats to the availability of communications are aimed at stopping the VoIP service are the type denial of service attacks (DoS - Denial of Service)., Whose main objective to make attacks on key elements of a VoIP communication system as proxy , gateway or client. The call attack flooding or flood calls, happens when an attacker aims to significantly reduce the performance of a system, either through the memory consumption, CPU or bandwidth, or even disable it. This attack can occur in a unified way, that is, from a single header, or distributed manner using botnet or coordinated attacks.

Another attack are the malformed messages. For this type of attack there are two ways to proceed. The first is to change the structure of a SIP message. The other is to maintain the regulated structure and then modify the default message content. The impacts to infrastructure can be infinite looping, buffer overflow, system failure, inability to process genuine messages, among others [2]. The call hijacking, or called sequestration, usually happens due to flaws in the authentication process between the parties involved in a VoIP communication. This is because the only user authentication by the server is commonly realized. The reverse process does not apply, allowing attackers through the man-in-middle attack if pass for legitimate servers.

B. Threats against Confidentiality:

The threats against the confidentiality cause no direct impact on communication between users, but can cause irreparable damage, considering that sensitive information can be intercepted and used for illicit purposes. The eavesdroping aims to gain access to calls in transit between users of a VoIP environment. Unlike difficulties to intercept a phone call on the PSTN (Public Switched Telephone Network),

VoIP environments this attack is very easy to perform, making If a frequent and popular threat [2], [7]. Attacks aimed at identity theft and passwords, are generally composed of a number of other attacks.

Initially, using a process of enumeration, the attacker performs a scan in the log server for Call-ID (user ID) valid fingerprints of devices and ports used, among others. Through improper access to control information easily obtained through an interception attack, an attacker can gain unauthorized access to identifiers that can provide information on destination/origin of calls, duration, content, registration servers, proxy gateways, among others.

C. Threats to Integrity:

The main objective of this type of threat is to commit connections in progress. This can be done by tampering signaling messages or else injection, substitution or deletion of information transmitted. Call forwarding is one of these attacks; can be any method or unauthorized attempt to redirect IP or a control message, in order to divert a call. The insertion and degradation of data from a VoIP communication can be made through sniffers tools, of the type attack man-in-the-middle, among others.

D. Threats against the Social Context:

Also categorized as social threats such threats have a different approach from the others. This because they lack technical nature, but rather on manipulating information in order to transform the attacking figure in an entity integrates and reliable. The misrepresentation or misrepresentation, refers to the act of providing false information to third parties as if they were true to a user or system can be duped [3].

Spam over IP Telephony (SPIT) is similar to the classic of spam emails. The spam over IP telephony is defined as the mass requests attempts set in order to establish a voice communication session or video [2]. When a victim answers the call or the call is forwarded to a voice mail, the spammer starts transmitting the message in real time. The vishing (phishing VoIP) is supported by other attacks and threats such as SPIT, misrepresentation of identity, content and authority. As in phishing, is to obtain personal information through illegal attempts usually confidential, the system users. The difference lies in the fact that vishing happens usually through voice calls or instant messages.

E. Related Work:

In order to better understand the threats that surround this environment, the use of honeypots has been proposed in recent years. In [7] the authors present a holistic approach to a system of detection and intrusion prevention, combining the use of a high-interaction honeypot VoIP and event correlation application layer SIP-based services. The architecture could use to detect multiple types of attacks such as DDoS, TIPS, among others.

The work done in [4] the authors present an implementation of the VoIP honeypot Artemis. The authors apply the honeypot in order to mitigate attacks as enumeration and SPIT and implement controls as collection devices vulnerable signatures and real-time control of security mechanisms. Developed to work exclusively in VoIP environments as a back-end user-agent, Artemis is a honeypot for the purpose of detecting malicious activity intended for this type of infrastructure, at an early stage. Real attack data collections are not made.

In [5] the authors describe a solution architecture deployed to intercept, analyze and report VoIP attacks. The presented solution implements a honeynet, based solely on the use of free software and systems like Asterisk PBX. The proposed architecture provides emulated services to attackers, ie, high-interaction honeypots are used to implement various real services in VoIP environments, in order to attract the largest number of possible attackers.

In [6] the same authors perform a VoIP system security assessment, based on analysis of information generated through the implementation of the honeynet from previous work [5]. The authors explain how the infrastructure of the honeynet was deployed and the analysis and evaluations of attacks suffered. In [8] and [9] the authors propose a VoIP honeypot that modifies the modus operandi of their implementation whenever it is necessary, in order to circumvent the maximum activity of an offender.

III. IMPLEMENTATION OF HONEYPOT

The implementation of the project took place from the installation and configuration of the honeypot low interactivity Dionaea [15]. The choice of this honeypot gave up due to its easy installation, configuration and maintenance, and can be implemented without major difficulties in a network. The server on which the honeypot was installed has the following settings:

- Processor: Intel (R) Core (TM) 2 Quad CPU Q9400 @ 2.66GHz
- RAM: 1 GB
- Operating System: GNU / Linux Ubuntu LTS 12:04:01
- Hard Drive: 80 GB

The honeypot was configured to be capable of emulating a SIP network, offering features such as components, services and SIP users. In addition, the honeypot has been configured with other services such as, ftp, http, mysql, among others, who served as bait for potential attackers to set up infrastructure. The honeypot is connected to the Internet via a dedicated connection of 1 Mbps, through which should be captured malicious activities transmitted on real traffic.

When called the software registers two important directories. The first is the / dionaea / etc /, where is located the dionaea.conf file,file that records all system settings. The second of them is / dionaea / var / directory, where are stored log files, other directories responsible for storing the data recorded by the honeypot and logsql.sqlite database file, responsible for the registration of all shares registered by the honeypot .

Subdirectories mentioned is important to highlight: / dionaea / var / binaries, where they recorded the binary malicious artifacts that were captured by the system; / dionaea / var / bistreams, responsible for registering the actions of the attackers on the honeypot and / dionaea / var / RTP, where the files relating to attempts to carry out fraudulent calls via SIP service (Fig. 1) is stored.

The honeypot was tested for robustness and accuracy. The purpose of these tests was to verify if the software deployed properly perform their tasks, such as capturing the attacks and storage of information in the

database. For this, they used network verification tools and simulation of traffic, such as SIPp and SIPScan. To test the robustness were generated approximately 50 simultaneous connections to the honeypot, which were sent through separate 100 messages per connection. In this way it was possible to verify the correct functioning of the honeypot even when subjected to a high amount of activity. The honeypot properly captured all the traffic generated and can then be operated to capture actual attacks.

IV. VOIP

VoIP is a wide technology that allows telephone calls to be made over computer networks like the Internet system. VoIP converts analog voice signals into digital data packets and supports real-time and multi transmission of conversations using Internet Protocol. VoIP calls can be made on the Internet by using a VoIP Service Provider and standard computer audio systems. Alternatively, some service providers support VoIP through ordinary telephones that use special adapters to connect to home computer network. Many VoIP implementations are based on the H.323 technology standard. VoIP offers an efficient cost savings over traditional long distance telephone calls. VoIP phone service may be less secure than ordinary phone service. Traditional phone lines can be wiretapped, but this requires physical access and installation effort. VoIP communications, on the other hand, can be investigated over the Internet electronically. Likewise, network attackers can interrupt your calls by interfering with the flow of data packets.

V. TERMINOLOGIES

We have introduced certain terminologies in the description of our models and for designing the VoIp architecture. The SIP network uses the components:

Entities interacting in a SIP scenario are called User Agents. User agents may operate in two way:

- User Agent Client (UAC)-It generate requests and send that requests to servers.
- User Agent Server (UAS)-It gets that requests, Processes on that request and generate responses.

A. Client:

In general we associate the knowledge of clients to the end user that is running on the system used by users.it may be softphones running on PC's or messaging device in IP phones. It generates a request when you try to call another person within a network and sends the request to a server.

B. Servers:

Servers are generally part of the network. They acquire a predefined set of rules to handle the requests sent by clients. There are several types of server:

1) SIP proxy server: This is most common type of server in a SIP environment. When request is generated by client, the exact address of the receiver is not known in previously. So, the client sends the request to a proxy server. The server on behalf of the client forwards the request to another proxy server or the recipient.
2) Redirect server: Redirect server redirects clients requests, to indicate that clients needs to choose different route to get the recipient.it happens when generally recipient has moved from its original location either temporarily or permanently.
3) Registrar: one of the vital jobs of the servers is to detect the location of a user within a network. User refreshes their location time to time by registering to a registrar server.
4) Location server: The address register in registrar server is stored in a location server.

VI. SYSTEM ARCHITECTURE

There are number of entities involve in VoIP system. User (sender and receiver) is usually authorised by SIP manager. Firstly, user sends credential for registration to SIP manager .Then SIP manger generates a SIP ID for each user to login the system. In this system only two authorized user can communicate to each other. When any user wants to send a message or want to communicate to other user, then it simply sends a request for connection. The proxy server accepts the request from the sender and forward it to SIP manager for checking authority of user. SIP manager have the database for user information, it also checks the user credential and sends response to server. If the authorized user is present then request is forwarded to the destination user otherwise request is not forwarded to destination.

If there is an attacker which want to hack the system or hijack the system. It sends the request for connection. At that time SIP manager checks the authentication of user and sends negative response to server. Server drops the call and save information of attacker in system like location, IP address etc. The security provided by honeypot for observing the traffic in network and detect the attacker. Honeypot uses to manage the traffic and provide security to user side data or information.

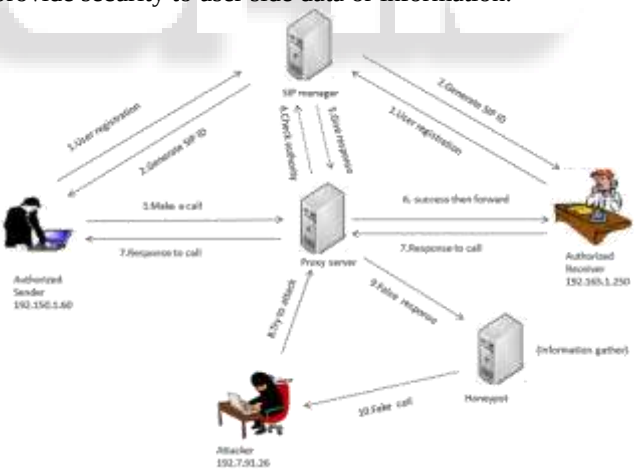

Fig. 1: System Architecture

In fig1 there are two authorized users which can communicate to each other but the third entity called attacker can't communicate to any user which is authorized by SIP. SIP manager detect the attacker and break the call as well as it store the information about attacker in backend. In this system the user use the smart phones, laptops, tabs, analogue phones personal computers etc for communication. Each user has unique username and password for login the system.

A. Registration and Authentication

In VoIP system user need to create an account with SIP manager using a unique identification criteria. Such a

system can include the IP address of user system, mobile number, location base information, user profile etc. Which unambiguously identifies the system or person. While setting up an account, SIP manager generate an SIP ID for each user, which is later used as login credentials for all users. SIP manger generate the SIP ID like email address for eg. If user is bob it send the credential for registration like user name, address, IP address of the systemic. Then SIP manager generate SIP ID like bob123@somewhere.com using this SIP ID bob login the system for communication.

B. Session Initiation Protocol

Session Initiation Protocol is the protocols used for setting up VoIP calls and is the crux of the IPTS. It is authority for initializing, modifying and tearing down sessions. The addressing for this sessions are based on Uniform Resource Identifiers of the involved parties and not the terminals that they are using SIP.SIP is the text based application layer protocol. Its syntax is similar to the Hypertext Transfer Protocol. It does not serve as a media gateway and it is solely responsible for the session setup/tear-down signalling. SIP doesn't define the media transfer protocol and it can be used over either TCP or UDP, and by default uses port number 5060. The parallaly of SIP to HTTP allows compatibility with web browser. The SIP message can be of any format, various types of information may be transmitted through SIP. It allow to contain messages from other protocols such as Real Time Protocol, Session Description Protocol, Resource Reservation Protocol (RSVP) and Real Time Streaming Protocol (RTSP).

SIP is decision making for determining the location of the end point to be used based on the Uniform Resource Identifiers (URI), with the help of a DNS server or intermediary proxies. Availability of users and their willingness to authorize the communication link is negotiated before a call is authorized and prior to the flow of information, Call initiations, holds, transfers, session termination are managed by SIP. A SIP server accepts requests from a User Agent Client and sends back responses. The server act as a proxy server, in which case it can act as a client and it forward requests to another server on behalf of a client. The server also works as a registrar, accepting checking, and REGISTER requests if the UAC is authorized to register with the network. The users can only make a call through a SIP proxy if user is registered. The SIP Proxy server forms a triangular topology with the client and user agent server. The proxy server receives requests from the User agent client (UAC), and decides where to forward that request. It may either forward it to User Agent Server or to another proxy. The response follows the same path in reverse. If the server finds multiple destinations for the requests, it can create the request and send it to all of them.

C. VoIP Conversation using SIP

The caller sends an INVITE message to the callee to initiate a multimedia session, for example a VoIP call. The callee may be answer with a "180 Ringing" message (provisional) and it must answer with a "200 OK" or error message. If there is no answer from the callee, the INVITE request will eventually time out. In order to tell the other party the specifications of the multimedia stream that will carry the actual voice signals, the caller has to embed an SDP message inside the SIP message's body.

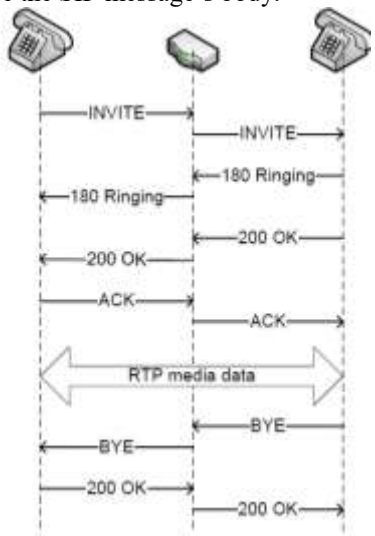

Fig. 2: VoIP conversation using SIP

He will also get an SDP message with parameters for the RTP stream from the callee. After the successful start of a session the media such as VoIP audio is sent using the Real-time Transport Protocol. The messages transmitted by each party in a typical VoIP session using SIP are shown in fig2.

A list of the most important, and often mandatory, SIP headers:

Header	Description
Via	Route of the packet
From	Public address of sender
To	Public address of receiver
Contact	Contact information of sender
Call-ID	Random ID of call session
CSeq	Request sequence number
Allow	Supported SIP requests
Max-Forwards	Maximum number of hops
Contant-Type	Type of body (e.g. SDP)
Content-Length	Length of body in bytes
User-Agent	Phone identifier (optional)

Some headers contain a random string that is used for identification purposes. Even though these additional random parameters are essential parts of the SIP specification, they are only discussed briefly because they are generated and processed by the exiting VoIP software used in this thesis. They do not play an important role in the concept of the proposed security architecture to be described in fig.

The additional random parameters are used to uniquely and globally identify call relationships. They are also important for detecting request loops in a network. For instance, the from header is of the form

From:

NAME <sip:EXTENSION@SERVER>;tag=RANDOM

with NAME being the full name or an alias of the person calling, EXTENSION being either the extension number or the nickname the caller is registered under on the VoIP server (given by SERVER), and RANDOM being a random alphanumeric string set by the calling phone. The To header can also contain such a random tag. The SIP protocol specifies that the tag is only to be used in peer to

peer dialogues and that is SIP requests and according responses.

Each request must contain one or more Via headers which must have a branch parameter appended to the address of the routing node. Therefore, a Via header is of the form

Via: SIP/2.0/UDP ADDRESS;branch=RANDOM

with ADDRESS being the network address of the node that forwarded and routed the request (including the original sender) and RANDOM being the random alphanumeric string that must always begin with the characters.

VII. ALGORITHM

A. Hash and FNV Hash Algorithm:

Hashes are used to assign some form of identify to a piece of information. The trick is that every time that information is hashed, it results in the same intimation. This is useful for tracking files to see if they've changed, or for using hash tables to store large sets of data.

Hash tables are used to store in coming packets in network. Some time there are traffic occurred in network that's effect on speed of data packets transmission and some time there may be data packet losses. To avoiding this problem we use algorithm. When traffic occurred in network that time data packets are store in hash table and then one by one send for destination. In this way we transfer the data packets without any losses.

1) FNV-1 Algorithm:

- hash = offset_basis
- for each octet of data to be hashed
- hash = hash * FNV_prime
- hash = hash Xor octet of data
- return hash

In the above pseudo code, all variables are unsigned integers. All variables, except for byte of data, have the same number of bits as the FNV hash. A variable, Byte_of_data, is an 8 bit unsigned integer.

As an example, consider the 64-bit FNV-1 hash:

- A variables, except for Byte_of_data, are 64-bit unsigned integers.
- Many variable, Byte_of_data, is an 8 bit unsigned integer.
- The FNV_offset_basis is the 64-bit FNV_offset_basis value: 1469598103.
- The FNV_prime is the 64-bit FNV_prime value: 1099511628211.
- The multiply returns the lower 64-bits of the product.
- The XOR is an 8-bit operation that change only the lower 8-bits of the hash value.
- The hash value return is a 64-bit unsigned integer.

2) FNV-1a Algorithm:

FNV 1a is a minor variation of FNV hash algorithm. The difference between the FNV1 and FNV 1a hash is the order of the Xor and multiply. The FNV 1a hash uses the FNV_prime and offset_basis.The FNV1 hash of the same n-bit size.

- hash = offset_basis
- for each octet of data to be hashed
- hash = hash Xor octet of data
- hash = hash * FNV_prime
- return hash

The above pseudocode has the same assumptions that were noted for the FNV-1 pseudocode. The minor change in order leads to much better avalanche characteristics.

B. Round Robin Algorithm:

Round robin is the scheduling algorithm used by the CPU during execution of the process. Round robin is designed for the time sharing systems. Round robin is similar to first come first serve scheduling algorithm. A round robin is an arrangement of choosing all the elements in a group in some rational order. From top to bottom of the list and then starting again at the top of the list. A small unit of time call as time slice or quantum is set/defined. All processes in the algorithm are kept in the circular queue called as ready queue. Each New process is added to the tail of the circular queue .Using this algorithm, CPU makes sure time slices are assigned to each process in equal portions or in circular order dealing with all process without any priority.

VIII. APPLICATIONS

The number of users of VoIP services is increasing every year. So, VoIP systems get more attractive for attackers. Therefore we introduce the system detecting an attacker using honeypot. Sometime data packets are loss during transmission because of collision occurs within a network .and this collision occurs by attacker to disturb the network. System avoid that problem by using hash table as well as handle the traffic and avoid data losses. The propose system use in multiple applications like military communication, VIP calls, Business related calls. Voice mail system. One of the application is Skype for VOIP calling.

For example, There are two military officer and they wants to communicate with each other on some security issues. But sometime their may be third entity can present called attacker.who trying to hack the data for illegal use. To avoid this attacking we use our system. In this system when two officer are communicate with each other then attacker can't hack the data because when attacker want to attack on the system. At that time SIP manager check the authentication of attacker and simply reject the connection as well as it store the information of attacker.

IX. FUTURE SCOPE

As future work can be done deploying a honeynet with sensors (honeypots) distributed geographically. This would provide the necessary range to in full Were registered 23 different user-agents. However, it was found by analyzing the recorded messages que some of these tools are variations of SipVicious tool. It can see also native user-agents of widespread softphone applications, such as eyeBeam, sipcli And Also the Asterisk Open Source PBX in its different versions and derivatives. Other tools originally developed for use by network administrators Were Observed Also, the sipsak and smap. The occurrence of unidentified user-agents Refers to more sophisticated attacks, through the use of more advanced tools.

The Obtained results allowed a more detailed look at the development of attacks Aimed at VoIP environments.

This information can be used to feed the rules of other security tools actions, such as firewalls and intrusion detection systems. The information Obtained Also can be used in the construction of blacklists and whitelists.

The research and implementations for this thesis concentrate on protecting the customers and users of the VoIP network. Parts of the infrastructure that are excluded from the security architecture are:

1) The protection of VoIP backend servers, that is proxies and registrars, however they might be used for collection of data,
2) Any computers and devices that are not within the protected network,
3) Physical security considerations, that is physical access control or TEMPEST, and
4) Individual protection mechanisms such as anti-virus products.

X. CONCLUSION

The number of solutions and users of VoIP systems have increased in recent years. This tendency makes them more attractive VoIP systems in the eyes of cybercriminals. This article has shown deploying a honeypot for the study of related attacks on the SIP protocol. It observed a series of attacks aimed at VoIP infrastructure, from initial attacks, as survey in search of SIP devices to attacks aimed at the total commitment of the infrastructure. Overall, the results led to a holistic view of the attacks carried out in the real world and the detection of various attacks and tools used to commit the attacks to the system can be concluded that there is potential for real VoIP systems. This information can be used to improve defense mechanisms and also help in developing a security policy for VoIP systems.

REFERENCES

[1] J. Matejk, O. Lábaj, J. and P. Londak Podhradsky. "VoIP Protection Techniques "52nd International Symposium ELMAR, Croatia, in 2010.
[2] P. Park. "Voice over IP Security" Cisco Systems, Inc; Cisco Press; Indianapolis, USA, 2009.
[3] VoIP SA. "VoIP Security Threat Taxonomy and Privacy" VOIPSA Public Release 1.0; 2005.
[4] R. Carmo, M. Nassar and O. Festor. "Artemis: an Open-Source Honeypot Back-End to Support Security in VoIP Domains "12th IFIP / IEEE International Symposium on Integrated Network Management 2011.
[5] M. Gruber, F. Fankhauser, S. Taber, C. and T. Schanes Grechenig. "Trapping and Analyzing Malicious VoIP Traffic Using the Honeynet Approach ", 6thInternational Conference on Internet Technology and Secured Transactions, Austria, in 2011.
[6] M. Gruber, F. Fankhauser, S. Taber, C. and T. Schanes Grechenig. "Security Status of VoIP Based on the Observation of Real-World Attacks on the Honeynet, "IEEE International Conference on Privacy, Security, Risk, and Trust, Austria, in 2011.
[7] M. Nassar, S. Niccolini, State R. and T. Ewald. "Holistic VoIP Intrusion Detection and Prevention System ", 1st International Conference on Principles, Systems and Applications of IP Telecommunications (IPTComm), 2007.
[8] C. Valli. "An Analysis of malfeasant Activity Directed at VoIP Honeypot ", Proceedings of the 8th Australian Digital Forensics Conference, 2010.
[9] C. Valli and M. Al-Lawati "Developing Robust VoIP Router Honeypots Using Device Fingerprints ", 1st International Cyber Resilience Conference, Australia, in 2010.
[10] D. Hoffstadt, A. Marold and E. Rathgeb, "Analysis of SIP-Based Threats Using the VoIP Honeynet System ", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, United Kingdom, in 2012.
[11] N. Provos and T. Holz. "Virtual honeypots: from botnet tracking to intrusion detection ", 1st edition, Upper Saddle River, New Jersey: Addison Wesley, 2007.
[12] A. Barfar and S. Mohammad. "Honeypots: Intrusion Deception," ISSA Journal, USA; 2007.
[13] The Honeynet Project & Research Alliance. "Know your enemy: Honeynets - What a honeynet is, its value, overview of how it works, and risk / issues involved ". Available in:http://old.honeynet.org/papers/honeynet/.
[14] A. Mairh, D. Barik, Jena D. and K. Verma. "Honeypot in Network Security:A Survey ", ACM International Conference on Communication, Computing & Security; India, IND 2011.
[15] Catches Bugs Dionaea. Available in: http://dionaea.carnivore.it/.

