VoIP Security Threat Taxonomy and Privacy

Prof. Arya Chandrapal Singh[1], Prof. Bhosale Sachin Bajirao[2]
Department of Computer Engineering,
Jaihind College of Engineering, Kuran,
Pune
aryanchandrapal@gmail.com[1]
ssachinbhosale@gmail.com[2]
khatrianand@gmail.com[3]

Prof. Khatri Anand Ashok[3]
Research Scholar
Shri.Jagdishprasad Jhabarmal Tibrewala University,Churela Jhunjhunu,Rajasthan

Abstract- The number of users of VoIP services is increasingevery year. Consequently, VoIP systems get 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 such as firewalls and intrusion detection systems.

Keywords*—Security, Honeypot, VoIP, SIP, Attacks.*

I.INTRODUCTION

Presently, the telecommunications universe is undergoing a change, with migration more and more constant auditory communication via circuits switched to auditory communication via scientific discipline network, conjointly called VoIP. This migration provides users a range of recent services and facilities within the case of VoIP communications one among the most difficulties area unit associated with security, with new attacks geared toward compromising a production setting. A system that suffered before, principally with attack on physical infrastructure, can currently take all threats directed to the protocol stack transmission control protocol / scientific discipline return too specific attacks targeted at voice protocols like SIP (Session Initiation Protocol), IAX (Intra-Asterisk Exchange) and RTP (Real-time Transport Protocol), among others.

SIP is one among the key VoIP protocols and has its design composed of 4 basic elements: user agent, SIP proxy, direct server and written record server. The user agent (UA) could be a logical operate that matches the design of the shopper. Accountable for initiating or replying to SIP transactions, will act as each shopper (UAC) and as a server (UAS), beginning SIP requests and SIP responses acceptive, or acceptive SIP requests and responsive them, severally.

Responsible for routing perform in an exceedingly SIP network, the SIP proxy is meant route the SIP requests and responses between the devices concerned, for the aim of finishing calls from UAC. The direct server aims to direct requests and responses supported SIP messages from category three hundred, directive the UAC to direct contact to the requested destination. However the registration server is to blame for registering data on any UA that has already logged on to the system. Furthermore because the development of alternative security part technology wasn't developed with a similar potency and speed dedicated to the delivery of applications and also the provision of the service. Consequently a spread of attacks on these systems have emerged (e.g. decision pursuit, data escape, decision handling, injection management codes). Despite having some data of those attacks, it's unattainable to collect consistent and reliable data regarding the ways, 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 infra-structure, 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. 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, i.e. 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.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 fashions:

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

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 .

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 the most common type of server in a SIP environment. When a request is generated by client,the exact address of the recipient is not known in advance. 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 client's requests to indicate that client 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 an 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.

IV. SYSTEM ARCHITECTURE

There are number of entities involve in VoIP system .User (sender and receiver) which is authorised by SIP manager. Firstly, user send credential for registration to SIP manager .SIP manger generate a SIP ID for each user for login the system. In this system only two authorized user can communicate to each other.

When user want to send message or communicate to other user it simply send request for connection..

The proxy server accept the request from sender and forward that to SIP manager for checking authority of user.SIP manager have the database for user information it checks the user credential and sends response to server.If there is authorized user is present then request forward to destination user otherwise request not forward to destination.

If there is an attacker which want to hack the system or hijack the system, It send request for connection.At that time SIP manager checks the authentication of user and send negative response to server.Server breaks 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.

In fig.1 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 have unique username and password for login the system.

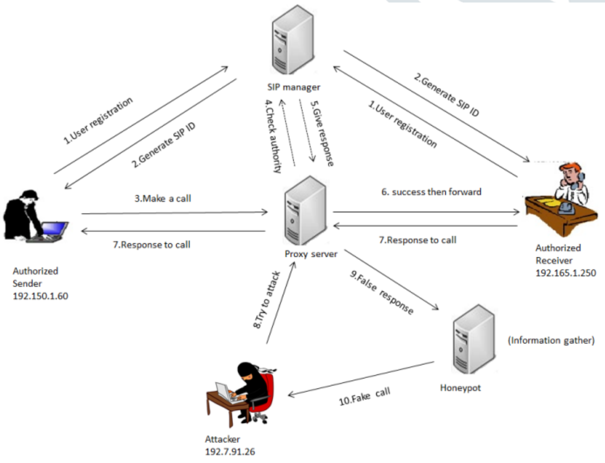

fig1.System Architecture

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 e.g. If user is bob it send the credential for registration like user name, address,IP address of the system etc. Then SIP manager generate SIP ID like bob123@somewhere.com using this SIP ID bob login the system for communication.

B. SESSION INITIATION PROTOCOL

The Session Initiation Protocol is the most popular 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 these sessions are based on Uniform Resource Identifiers (URI) of the involved parties and not the terminals that they are using SIP.SIP is a text based application-layer protocol, and its syntax is very similar to the Hypertext Transfer Protocol (HTTP). It does not serve as a media gateway and is solely responsible for the session setup/tear-down signaling. SIP does not define the media transfer protocol; 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 browsers. The SIP message can be of any format, various kinds of information may be transmitted trough SIP. It allow to contain messages from other protocols such as Real Time Protocol (RTP), Session Description Protocol (SDP), 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 and 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, transfers, holds, and session termination are all managed by SIP. A SIP server accepts requests from a User Agent Client (UAC) and sends back responses. The server may act as a proxy server, in which case it can act as a client and forward requests to another server on behalf of a client. The server also functions as a registrar, accepting REGISTER requests, and checking if the UAC is authorized to register with the network.The user can only make a call through a SIP proxy if he/she is registered. The SIP Proxy server forms a triangular topology with the user agent server and client as shown in Figure 5 [12]. The proxy server receives requests from the User agent client (UAC), and decides where to forward that request. It may either forward it to a User Agent Server (UAS) or to another proxy. The response follows the same path in reverse. In case the server finds multiple destinations for the requests, it can fork the request and send it to all of them.

VOIP CONVERSATION USING SIP

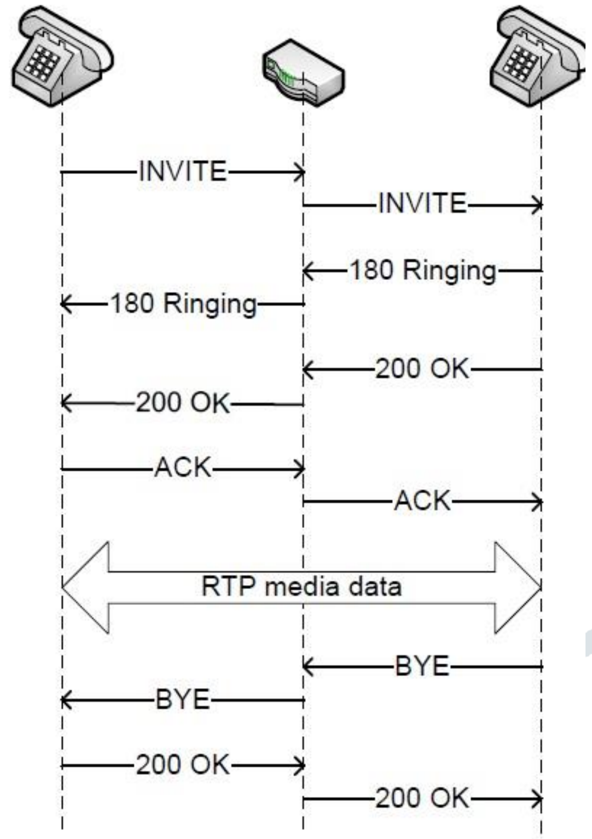

Fig2:VoIP conversation using SIP

The caller sends an INVITE message to the callee to initiate a multimedia session, forexample a VoIP call. The callee may answer with a “180 Ringing” message (provisional)and must answer with a “200 OK” or error message. If there is no answer from thecallee, the INVITE request will eventually time out. In order to tell the other party thespecifications 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. He will also get an SDPmessage 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 theReal-time Transport Protocol. The messages transmitted by each party in a typical VoIPsession 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
Content-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. Eventhough these additional random parameters are essential parts of the SIP specification,they are only discussed briefly because they are generated and processed by the exitingVoIP software used in this thesis. They do not play an important role in the concept of theproposed 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 beingeither the extension number or the nickname the caller is registered under on the VoIPserver (given by SERVER), and RANDOM being a random alphanumeric string set by thecalling phone. The To header can also contain such a random tag. The SIP protocolspecifies that the tag is only to be used in peer-to-peer dialogs that are SIP requests andaccording responses.

Each request must contain one or more via headers which must have a branch parameterappended 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 therequest (including the original sender) and RANDOM being a random alphanumeric stringthat “MUST always begin with the characters z9hG4bK” (section 8.1.1.7 [27]).

V. ALGORITHM

A. The redirection algorithm:

The redirection algorithm performs the per-flow treatment of each flow in the Flow

List (FL) in a time window at POP. The pseudo code is as follows:

```
HoneypotControllerPerFlow (FL)
 For a flow in FL
If (Tag = attack)
Parse the primary packet and search source and
destination address (FDA andFSA)
 PDA = FDA
 NDA = PDA
A: If (NDA = Destination address of honeypot)
 Forward the packet to NDA
Else
Replace NDA by destination address of honeypot
 Forward the packet to NDA
If (More Fragment = 0)
Goto S
 Else
 Parse next header of the flow for PDA
 NDA = PDA
 If (Tag = attack)
Goto A
 Else
Goto B
 Else
 Parse the primary packet and search source and
destination address (FDA and
FSA)
```

```
 PDA = FDA
 NDA = PDA
 B: If (NDA = Destination address of active FTP server)
 Forward the packet to NDA
 Else
 Replace NDA by destination address of server
 Forward the packet to NDA
 If (More Fragment = 0)
Goto S
 Else
parse next header of the flow for PDA
 NDA = PDA
 If (Tag = attack)
Goto A
 Else
Goto B
 S: Stop
```

VI. APPLICATIONS

The number of users of VoIP services is increasing every year. VoIP systems get more attractive for attackers.Therefore we introduce the system detecting an attacker using honeypot.Sometime data packets are loss during transmissions because of collision occurred within a network .and this collision occur 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 most commonly use 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 there 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 than attacker can't hack the data because when attacker want to attack on the system at that time SIP manager check the authority of attacker and simply reject the connection as well as it store the information of attacker.

VII. ADVANTAGES

- Maintaining low collision rate.
- Improve the performance of network.
- Provide short response time.
- Cost reduction
- Confidentiality: data must only be accessible to authorised parties.
- Integrity: data must not be modified by unauthorised parties
- Availability: data must be available at all times
- Authenticity: ability to verify the identity of a user

VIII. FUTURE SCOPE

As future work can be done deploying a honeynet with sensors (honeypots) distributed geographically. This would provide the necessary range toIn full Were registered 23 different user-agents. However, it was found by analyzing the recorded messages queue some of these tools are variations of Sip Vicioustool. 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 and shouldn't 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 theymight 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.

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 ProtectionTechniques "*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 PublicRelease 1.0; 2005.*

[4] R. Carmo, M. Nassar and O. Festor. "Artemis: an Open-Source HoneypotBack-End to Support Security in VoIP Domains "*12th IFIP / IEEEInternational 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 HoneynetApproach ", *6thInternational Conference on Internet Technology and SecuredTransactions, Austria, in 2011.*

[6] M. Gruber, F. Fankhauser, S. Taber, C. and T. Schanes Grechenig. "SecurityStatus of VoIP Based on the Observation of Real-World Attacks on theHoneynet, "*IEEE International Conference on Privacy, Security, Risk, andTrust, Austria, in 2011.*

[7] M. Nassar, S. Niccolini, State R. and T. Ewald. "Holistic VoIP IntrusionDetection 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 VoIPHoneypot ", *Proceedings of the 8th Australian Digital Forensics Conference,2010.*

[9] C. Valli and M. Al-Lawati "Developing Robust VoIP Router HoneypotsUsing Device Fingerprints ", *1st International Cyber Resilience Conference,Australia, in 2010.*

[10] D. Hoffstadt, A. Marold and E. Rathgeb, "Analysis of SIP-Based ThreatsUsing the VoIP Honeynet System ", *IEEE 11th International Conference onTrust, Security and Privacy in Computing and Communications, United Kingdom, in 2012.*

[11] N. Provos and T. Holz. "Virtual honeypots: from botnet tracking tointrusion detection ", *1st edition, Upper Saddle River, New Jersey: AddisonWesley, 2007.*

[12] A. Barfar and S. Mohammad. "*Honeypots: Intrusion Deception," ISSAJournal, USA; 2007.*

[13] The Honeynet Project & Research Alliance. "Know your enemy:Honeynets - What a honeynet is, its value, overview of how it works, andrisk / 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/.