ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 3, March 2016

A Survey on VoIP Attack Detection by using Honeypot

Supriya B. Kurhade[1], Chaitali B. Palwe[2], Priyanka R. Pande[3], Prof. A. V. Kanade[4]

BE Students, Dept. of Computer, Jaihind College of Engg., University of Pune, India[1,2,3]

Assistant Professor, Dept. of Computer, Jaihind College of Engg., University of Pune, India[4]

ABSTRACT*:* The number of users of VoIP services is increasing every 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, Skype, Attacks.

I.INTRODUCTION

A unified system of communications using a VoIP business communication system, will modify communications and increase productivity across your organization. A VoIP communication system will be designed to fulfill a spread of business functions, including: simultaneous telephony reception across multiple devices, transcription of emails into voicemails, and also the ability to fulfil significant decision volume while not being compromised like regular phone lines. VoIP phone systems will ring across multiple devices, even mobile devices, keeping workers connected with coworkers and clients. And, if you ever do miss that decision, it will transcribe voicemails into emails, thus you'll make sure message although you're still on the phone!

Presently, the telecommunications universe is undergoing a modification, with migration additional and additional constant auditory communication via circuits switched to communication via subject network, collectively known as VoIP. This migration provides users a variety of recent services and facilities among the case of VoIP communications one of the foremost difficulties square measure related to security, with new attacks double-geared toward compromising a production setting. A system that suffered before, chiefly with attack on physical infrastructure, will presently take all threats directed to the protocol stack transmission control protocol / subject 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.

II. 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. VOIP SECURITY

Threats to VoIP environments security comprise the full of the issues faced by information networks, more specific issues of integrated protocols and services to a VoIP infrastructure [7]. With relation to threats meant for environments with VoIP infrastructure, there square measure various ways that to categorise 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 square measure geared toward stopping the VoIP service square measure the kind denial of service attacks (DoS - Denial of Service)., Whose main objective to create attacks on key parts of a VoIP communication system as proxy , entree or shopper. the decision attack flooding or flood calls, happens once associate degree assailant aims to considerably scale back the performance of a system, either through the memory consumption, processor or information measure, or maybe disable it. This attack will occur in an exceedingly unified means, that is, from one header, or distributed manner mistreatment botnet or coordinated attacks.

Another attack square measure the distorted messages. For this kind of attack there square measure 2 ways that to proceed. the primary is to alter the structure of a SIP message. the opposite is to take care of the regulated structure so modify the default message content. The impacts to infrastructure will be infinite process, buffer overflow, system failure, inability to method real messages, among others [2]. the decision hijacking, or referred to as sequestration, sometimes happens attributable to flaws within the authentication method between the parties concerned in an exceedingly VoIP communication. this is often as a result of the sole user authentication by the server is often realised. The reverse method doesn't apply, permitting 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, however will cause irreparable harm, considering that sensitive data will be intercepted and used for illicit functions. The eavesdroping aims to achieve access to calls in transit between users of a VoIP surroundings. not like difficulties to intercept a telephony on the PSTN (Public Switched phonephone Network), VoIP environments this attack is incredibly straightforward to perform, creating If a frequent and common threat. Attacks geared toward fraud and passwords, square measure usually composed of variety of different attacks.

Initially, employing a method of enumeration, the assailant performs a scan within the log server for Call-ID (user ID) valid fingerprints of devices and ports used, among others. Through improper access to regulate data simply obtained through associate degree interception attack, associate degree assailant will gain unauthorized access to identifiers that may offer data on destination / origin of calls, duration, content, registration servers, proxy gateways, among others.

C. Threats to integrity:

The most objective of this type of threat is to commit connections in progress. this will be done by tampering signaling messages alternatively injection, substitution or deletion of data transmitted. call forwarding is one in every of these attacks; is any technique or unauthorized attempt to send information processing or a control message, so as to divert a call. The insertion and degradation of information from a VoIP communication is created through sniffers tools, of the type attack man-in-the-middle, among others.

IV. WHY WE USE SKYPE

IP telecommunication is gaining popularity for sure and shortly it will challenge the modern telecommunication system. VoIP (Voice over IP) is cheaper and has sound quality that is improving with every passing day. it's simple to remember anybody's VoIP user id than his lengthy phone number and once comes, the popularity and demand the competition begins. SIP and Skype are not only 2 VoIP service providers however are 2 different technologies altogether. they are serving the same to the users worldwide however the technological approach of each of those players is entirely totally different.

SIP is Public and Skype is private. yes that's true – SIP may be a technology standard developed by internet Engineering Task Force. It only handles the user's location on the internet, users authentication, call handling and telephone.On the other hand Skype will everything on its own without victimization any of the protocols defined by IETF. however is finished and what technique is used stays a secret because Skype is private company and has not disclosed its technology yet.Skype is an application that provides video chat and voice call services. Users might exchange such digital documents as pictures, text, video and any others, and may transmit each text and video messages. Skype permits the creation of video conference calls. Skype permits users to speak over the net by voice employing a microphone, by video by using a digital camera, as well like instant messaging.

V. System architecture

There are variety of entities involve in VoIP system .User (sender and receiver) that is authorised by server. Firstly, user send credentials for registration to admin. Admin generate a user ID for every user for login the system. during this system only 2 authorized user will communicate to each other.When user need to send message or communicate to other user it simply send request for connection.The proxy server accepts the request and checks the authority of user. Server has the information for user data it checks the user credentials and sends response to client. If there's authorized user is present then request forward to destination user otherwise request not forward to destination.

If there's an attacker that want to hack the system or hijack the system, It send request for connection .At that time server checks the authentication of user and send negative response to server. Server breaks the call and save data of attacker in system like location, information processing address etc. the safety provided by honeypot for observing the traffic in network and find the attacker. honeypot uses to manage the traffic and provide security to user side information or data.

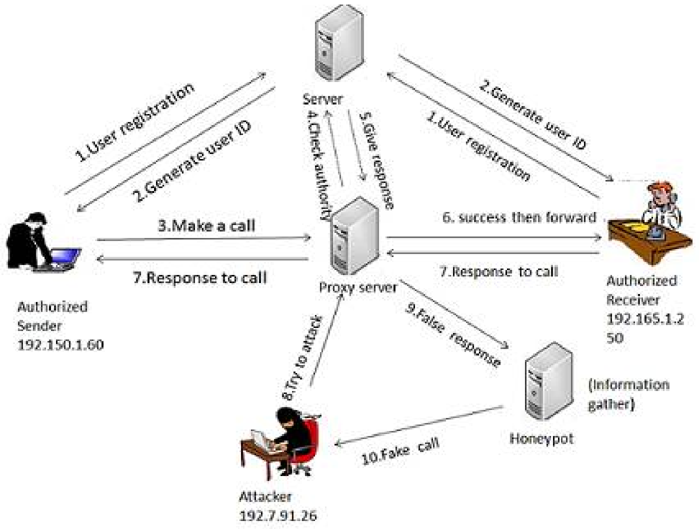


Fig. System Architecture

In fig. there are 2 authorized users which can communicate to each different however the third entity known as attacker can’t communicate to any user that is authorized by server. Server find the attacker and break the decision as well as it store the information regarding attacker in backend. during 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.

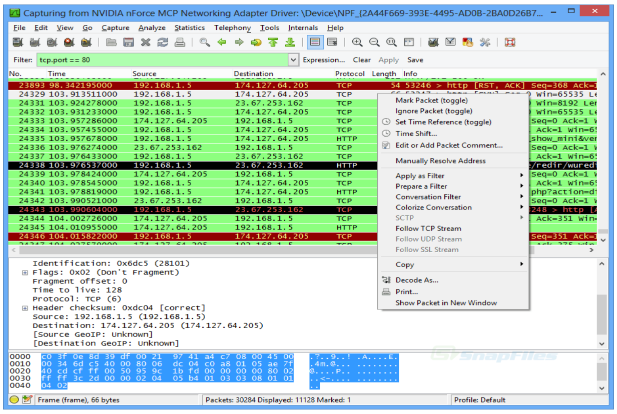
A. *Registration and Authentication In*

VoIP system user need to create an account with server using unique identification criteria. Such a system will include the information processing address of user system, mobile number, location base data, user profile, waterproof address of the system etc. This unambiguously identifies the system or person. whereas setting up an account, server generates an user ID for each user, which is later used as login credentials for all users.
Authentication is one in all the most important tasks in our system. Server provides authority to user for communication. when user send a request for participation|asking|letter of invitation|missive of invitation} for call, then system check all credential of user for authentication. If any authorised person makes a call then it with success send to destination. Otherwise call forward to honeypot system.

B. *Packet Capturing*

In system, we use wireshark is used for packet capturing. This helps for tracking the packet and observes the traffic in network. it's used for network troubleshooting, analysis, software and communications protocol development, and education. It capture information like senders and receivers information processing address, transmission time of packet, protocol used for packet transmission, and data regarding packet etc.Wireshark is a free ,open source debugging tool.wireshark is an advanced packet analysis tool that is used for HTTP traffic analysis as well as the other network traffic, like debugging information processing phones.

Wireshark is a network packet analyzer.a network packet analyzer will try to capture network packet and tries to display that packet data as detailed as possible.you could think of a network packet analyzer as a measuring device used to examine what’s going on inside a network cable, just like a voltmeter used by an electrician to examine whats going on inside an electric cable(But at a higher level , of course).



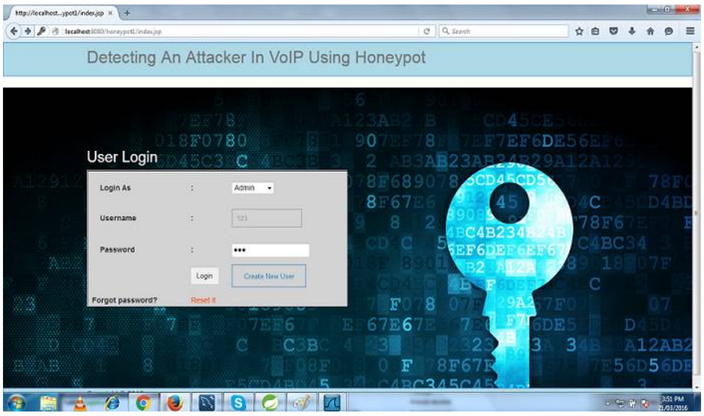
Filter: tcp.port == 80

```
No.    Time              Source           Destination      Protocol Length  Info
23893 98.342195000   192.168.1.5      174.127.64.205   TCP      54 53246 > http [RST, ACK] Seq=368 Ack=
24329 103.913511000  192.168.1.5      174.127.64.205   TCP                        win=65535 Le
24331 103.924278000  192.168.1.5      23.67.253.162    TCP                        win=8192 Len
24332 103.931233000  192.168.1.5      174.127.64.205   TCP                        win=65535 Le
24333 103.957286000  174.127.64.205   192.168.1.5      TCP                        Seq=0 Ack=1 w
24334 103.957455000  192.168.1.5      174.127.64.205   TCP                        Ack=1 Win=6
24335 103.957678000  192.168.1.5      174.127.64.205   HTTP                       show_mini&ver
24336 103.976274000  23.67.253.162    192.168.1.5      TCP                        Seq=0 Ack=1 w
24337 103.976433000  192.168.1.5      23.67.253.162    TCP                        Ack=1 Win=6
24338 103.976537000  192.168.1.5      23.67.253.162    HTTP                       /redir/wured
24339 103.978424000  174.127.64.205   192.168.1.5      TCP                        Seq=0 Ack=1 w
24340 103.978545000  192.168.1.5      174.127.64.205   TCP                        Ack=1 Win=6
24341 103.978819000  192.168.1.5      174.127.64.205   HTTP                       php?action=d
24342 103.990521000  23.67.253.162    192.168.1.5      TCP                        Seq=0 Ack=1 w
24343 103.990604000  192.168.1.5      23.67.253.162    TCP                        248 > http [
24344 104.002726000  174.127.64.205   192.168.1.5      TCP                        Ack=351 Win=
24345 104.010955000  174.127.64.205   192.168.1.5      HTTP
24346 104.015822000  192.168.1.5      174.127.64.205   TCP                        Seq=351 Ack=
```

```
    Identification: 0x6dc5 (28101)
  ⊞ Flags: 0x02 (Don't Fragment)
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊞ Header checksum: 0xdc04 [correct]
    Source: 192.168.1.5 (192.168.1.5)
    Destination: 174.127.64.205 (174.127.64.205)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```

```
0000  c0 3f 0e 8d 39 df 00 21  97 41 a4 c7 08 00 45 00   .?..9..! .A....E.
0010  00 34 6d c5 40 00 80 06  dc 04 c0 a8 01 05 ae 7f   .4m.@... ........
0020  40 cd cf ff 00 50 95 9c  1b fd 00 00 00 00 80 02   @....P.. ........
0030  ff ff 3c 2d 00 00 02 04  05 b4 01 03 03 08 01 01   ..<-.... ........
0040  04 02                                              ..
```

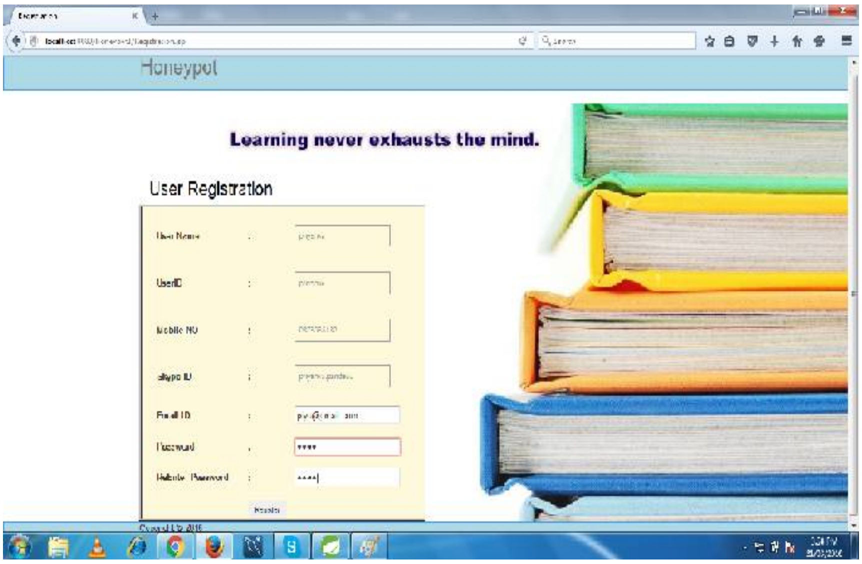
Frame (frame), 66 bytes | Packets: 30284 Displayed: 11128 Marked: 1 | Profile: Default



Detecting An Attacker In VoIP Using Honeypot

User Login

Login As	:	Admin
Username	:	123
Password	:	•••

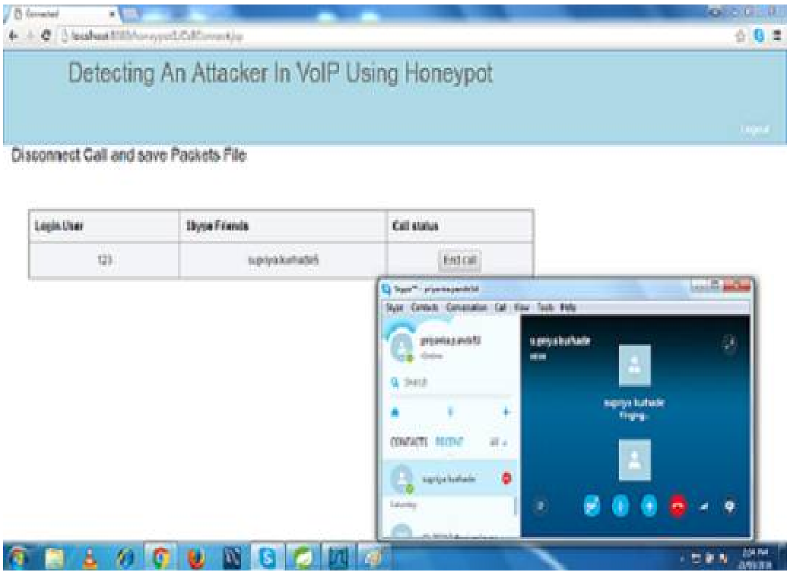


Honeypot

Learning never exhausts the mind.

User Registration

User Name	:	[illegible]
UserID	:	[illegible]
Mobile NO	:	[illegible]
Skype ID	:	[illegible]
Email ID	:	[illegible]
Password	:	••••
Website Password	:	••••



Detecting An Attacker In VoIP Using Honeypot

Disconnect Call and save Packets File

Login User	Skype Friends	Call status
123	supriyakurhade	End call

VI. ALGORITHM

We are using Modified Source Based Filtering (MBSF)algorithm for your project to filter the packets to prevent the attack.

Steps of Algorithm:

1. Calculate hop_count m from the TTL field of the received packet.
2. If the normal statistics bm is 0, discard the packet as a attack packet and be over.
3. Carry out the statistics in terms of the segment values of the IP address.
4. If bm>am, be over
5. Score the packet according to the intensity. If the intensity holds, the packet is discarded.

bm is current profile or state of hop
am is nominal profile or sate of hop

VII. APPLICATION

The number of users of VoIP services is increasing each year. VoIP systems get a lot of attractive for attackers. so we have a tendency to introduce the system detecting an attacker exploitation honeypot. someday information packets are loss throughout transmissions because of collision occurred inside a network .and this collision occur by attacker to disturb the network. system avoid that drawback by exploitation hash table as well as handle the traffic and avoid information losses. The propose system use in multiple applications like military communication, VIP calls, Business connected calls. Voice mail system.one of the foremost usually use application is Skype for VOIP calling.

For example, There are 2 military man and that they wants to speak with one another on some security problems. however someday there may be third entity will present known as attacker, who attempting to hack the info for illegal use. To avoid this attacking we use our system. during this system once 2 officer are communicate with one another than attacker can't hack the info because once attacker want to attack on the system at that point SIP manager check the authority of attacker and easily reject the connection likewise because it store the information of attacker.

VIII. ADVANTAGES

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

IX. CONCLUSION

The number of solutions and users of VoIP systems have increased in recent years. This tendency makes them a lot of attractive VoIP systems within the eyes of cybercriminals. this text has shown deploying a honeypot for the study of related attacks on the SIP protocol. It observed a series of attacks aimed toward VoIP infrastructure, from initial attacks, as survey in search of SIP devices to attacks aimed toward the total commitment of the infrastructure. Overall, the results led to a holistic of the attacks carried out within the world and therefore the detection of varied attacks and tools used to commit the attacks to the system is finished that there's potential for real VoIP systems. This data is used to improve defense mechanisms and additionally facilitate in developing a security policy for VoIP systems.

REFERENCES

1. J. Matejk, O. Lábaj, J. and P. LondakPodhradsky."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 Public Release 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 / IEEE International Symposium on Integrated Network Management 2011*.
5. M. Gruber, F. Fankhauser, S. Taber, C. and T. SchanesGrechenig."Trapping and Analyzing Malicious VoIP Traffic Using the HoneynetApproach ", *6thInternational Conference on Internet Technology and Secured Transactions, Austria, in 2011*.
6. M. Gruber, F. Fankhauser, S. Taber, C. and T. SchanesGrechenig."SecurityStatus of VoIP Based on the Observation of Real-World Attacks on theHoneynet, "*IEEE International Conference on Privacy, Security, Risk, and Trust, 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 on Trust, Security and Privacy in Computing and Communications, United Kingdom, in 2012*.

BIOGRAPHY

Kurhade Supriya,Palwe Chaitali and Pande Priyanka are BE Students and **Prof**.**Amrut kanade** the Assistant Professor in the Computer Engineering Department, Jaihind College of Engineering(Pune), SavitribaiPhule,Pune.