Forensic Analysis of Asterisk-FreePBX based VoIP Server

Hardik Tandel, Parag H. Rughani, Ph. D.*
IFS, Gujarat Forensic Sciences University,
Gujarat, India

Abstract—

VoIP – Voice over IP is becoming an important aspect of communication. With invention of high speed Internet together with mobile phones has made it possible to utilize this highly important technology for voice communication. International calls are now possible with VoIP at compatible rates compared to past. The trend made people develop applications based on VoIP not only for private IP PBX but for subscribed users from all over the world. The dependency in whole technology is its VoIP Server, which is not directly exposed to end users, but if can be compromised then can affect all the connected users. Looking at increasing popularity of VoIP, attackers are now targeting these VoIP servers for various purposes like stealing information or using service to make free calls. It is always difficult to prevent such attacks but investigation may always help in solving such attacks and preventing future attacks with similar modus operandi. These work focuses on forensic analysis of VoIP server asterisk and discusses important artifacts which can be retrieved from affected VoIP server.

Keywords—VoIP Forensics, Asterisk Forensics, FreePBX Forensics, Asterisk Analysis, VoIP Analysis, VoIP Attacks, VoIP related crimes

I. INTRODUCTION

VoIP is a revolutionary word that has changed ways of communication. It is one of the most crucial invention Internet users are utilizing but are least aware about it. People are enjoying VoIP calling but are not technically aware about change it has brought in the communication industry. Some of the interesting findings show interesting facts. It has been observed that companies switching to VoIP save between 50 to 70 percent [1], Unified Communications saves around 115 minutes a day per employee [2], the market of Global VoIP Services to Surge from USD 83 Billion in 2015 to USD 140 Billion by 2021 [3], telecoms are losing an average of 700,000 landline customers per month [4], By 2018, 42 percent of firms will send 100 percent of their traffic over SIP trunks [5], and much more [6].

The VoIP is certainly a very useful medium of communication but is it secure enough to communicate and store personal information? The answer is of course a subjective statement and it would vary based on the security implementation. However, it has been observed in most of the cases that companies implementing VoIP do not customize default solutions and do not emphasize on security. Main reason could be lack of awareness about possibilities of cyber attacks on this technology. Nevertheless, this is also not an untouched area and attacks have already been observed on VoIP setups.

Researchers have already warned about increasing attacks on VoIP [7][8], some of the authors have found and explored common vulnerabilities in VoIP environment [9]. This is one of the expected things which happen in the cyber world, as soon as new technology become popular, attackers start targeting it. Due to lack of awareness and security experts it is difficult to stop the attacks on VoIP environment. But, proper investigation is required to make sure criminals are punished. As the technology is emerging, very few forensic investigators are well versed in handling cases related to VoIP. The work mentioned in this paper is carried out to assist such forensic investigators in solving VoIP related crimes.

II. RELATED WORK

As being an old concept, sufficient research is done on VoIP technology, security and forensics. Some of the relevant articles are cited here. Some researchers worked on VoIP client [10], while some researchers focused on VoIP networks [11][12], some focused on attack patterns [13][14], while some emphasized on forensics aspects [15][16]. However, different researchers worked on enhancing security and forensics practice for VoIP attacks, there is still much to do in this field. This article is based on forensic analysis of Asterisk and FreePBX to make forensic investigators understand important artifacts, which can be retrieved from a VoIP environment.
III. EXPERIMENT

This section discusses experiment carried out to achieve objective. Asterisk server is selected at the core for setting up VoIP environment. The reasons behind selecting asterisk server are its openness, power and popularity [17]. The server as being open source allows all sorts of customization in setting up private IP PBX in any enterprise [18]. Front end is required to manage asterisk server which comes as a module with asterisk is FreePBX [19]. The solution offered by asterisk with FreePBX can allow any small to large organization to setup a low cost private IP PBX with minimum inputs. FreePBX provides a reach and user friendly GUI to asterisk, which makes it easy for administrators to configure VoIP Server as per the requirement [21].

After setting up the server, various users had been created to see real time communication. Soft Phone Zoiper [22] was used as a client. Calls were made to different extensions to create log entries at server. A custom shell script to use tcpdump [23] for capturing packets was written and same was used for network traffic interception. After sufficient entries, Forensic Falcon disk imager [24] was used to create image of the Server Hard Disk having Asterisk. EnCase Forensic [25] was used to analyze image and understand important artifacts from the disk. Observations are discussed in following section.

IV. RESULTS

Crucial artifacts were found while analyzing hard disk dump using encase. Some of the important artifacts are mentioned below:

A. List of users [Extensions and Passwords] were retrieved from the dump.

![Fig. 4.1 Users and Passwords](image)

Above detail is very useful in getting basic idea about various users who had been created to access the asterisk server. Apart from username and password it also shows email ID and other account related details. However, only user detail is not sufficient in investigating a case. There is need to identify calls related details. CDR details plays a crucial role in investigating a crime, fortunately we could find following details related to calls made using asterisk.

B. CDR Details were recovered from a comma separated file called Master.csv located on /var/log/asterisk/cdr-csv as shown below:

The detail shown in above figure gives a complete insight about calls made using asterisk server. The csv file includes majority of critical information including username, extension, duration of the call, status of the call and much more.
After getting call details, it is required to understand and learn about the VoIP client and content of the call. As mentioned earlier a custom shell script based on tcpdump was created to intercept packets from asterisk server. Packets captured using this script was analyzed using wireshark and it was possible for us to find out client details and listen the communication carried out by user through asterisk based VoIP.

C. VoIP Client detail was retrieved from the captured packet. The analysis was done using wireshark as shown below. As mentioned earlier zoiper was used to make the calls. Detailed analysis of the packet allowed us to find out IP address from where the call was made, related time stamps and client details as shown in following figure.
D. After getting VoIP client details, we focused on finding out voice data communicated over VoIP. The captured packets helped in achieving this as shown below.

![Fig. 4.4 Voice Content – RTP](image)

Next, we could retrieve crucial logs related to access and error. However, it is common to analyze these logs in routine computer forensics, but in case of VoIP related crimes, these log files can reveal much more. These logs play crucial role when a VoIP server was attacked remotely or a compromised VoIP server was used to change certain system level settings or credentials.

E. Access Logs are very important in understanding who accessed web server at what time and from where. Following screen depicts part of access log retrieved from our experiment.

![Fig. 4.5 Access Logs](image)
F. Similar to access logs, error logs are equally important as they log all the errors raised on the server. Following screen is a part of error log retrieved from our experiment.

![Error Log](image)

The observations shown above are few related to basic analysis of a crime committed using or targeting an asterisk server. They include almost all the basic things an investigator should know for investigating such crimes. The details mentioned in this article makes forensic investigator familiar about important artifacts of asterisk server.

V. CONCLUSION

Outcome of the work will assist forensic investigators who are not very comfortable with VoIP server investigation. It is worth as most of the VoIP solutions - commercial or free - have asterisk at their core. This article will act as a basic guideline for the investigators and they can take help of findings of this paper to speed up their investigation.

REFERENCES


[5] SIP trunking statistics that show how fast IT managers are making the transition, ExpertIT, 2013


