Analysis of VoIP based Network Content from Deep Packet Inspection

Ritu Dahiya
Department of Computer Science
Kadi Sarva Vishwavidyalaya, Gandhinagar

Dr. Jagdishchandra G. Pandya
Department of Science and Technology, Government of Gujarat,
Nr. Ch-0 Circle, Indulal Yagnik Marg, Gandhinagar-382007

Abstract- In this research an analysis of Session Initiation Protocol (SIP) is performed. SIP is a widespread Voice over IP (VoIP). Packet capture of volatile stream VoIP data and its analysis is carried out in order to investigate for identifying suspicious caller. The simulation was done on real time attack scenario and the findings were encouraging. It proves that, if appropriate forensic investigation steps are applied, potential evidences can be obtained. The type of end point user, equipment of the internal users, third party applications, the virtual private network and the software that are used to build reliable information are discussed. [1] On the other hand the virtual private network IP address of the suspicious attacker is identified even during the presence of VoIP services.

Keywords– VoIP, Packet Analysis, Forensic, Real Time Protocol

I. INTRODUCTION

The convergence of multimedia and data networks has resulted in increased network related crimes. Real-time feature of voice calling is required on the network for certain applications. VoIP is sensitive to the latency and jitter properties of the network due to which the users quickly perceive such problems and raise trouble tickets when they experience them. [2] The web server transactions and email traffic have a comparatively higher tolerance for latency and jitter. To manage the additional complexity of VoIP effectively, deployments offer significant benefits to IT personnel by:-

Trouble ticket reduction & Maintaining a higher level of user satisfaction.

A comprehensive management strategy requires alignment along with organizational processes and consistency in managing the entire application's delivery lifecycle. Some of the examples include detailed plans for deployment, troubleshooting, network maintenance and upgrades. [4] Implementing the process in each part of the lifecycle is the use of the management tools that aid in planning, managing and troubleshooting enterprise networks.

II. BACKGROUND STUDY

The two type of telephone systems - VoIP & PSTN [3] are considered for this paper and mentioned in this section.

Voice over Internet Protocol (VoIP)

VoIP is applied for delivering multimedia & voice sessions over Internet Protocol. Here, voice signals are converted into digital signals that makes them transferable over Internet Protocol. The analog call is converted into digital. The digitized call is compressed and translated into IP packets for transmission over IP network. [5] It is packet switched, meaning that the signals are divided into packets, which travel via dynamic routing up to the sink. The greatest benefit of this property is that bandwidth efficiency is greatly enhanced as compared to circuit switching. VoIP service begins with calls between two parties on separate computers. The most popular ones are as follows:-

Scenario 1: PC ↔ PC

Users connect to an IP network through a computer in this scenario. It has become very popular over the last years due to introduction of applications like Skype, Messenger etc. Many VoIP providers offer their services free of charge within its own network for personal use & in gaming industry. This scenario is referred to as VoIP, which will not be the covered in this paper.

Scenario 2: IP phone ↔ IP

Phone works the same way as scenario 1, but unlike it, the users need special IP phones. For the previous scenario, VoIP providers often offer service free of charge within their own network. When individuals and enterprises purchase VoIP service from providers, it is known as managed VoIP. Managed VoIP will be examined in this paper. Reliable telecommunication service i.e. QoS is expected. The service provider will provide the equipment, software etc.

Scenario 3: IP phone/PC ↔ PSTN

After the success of both previous scenarios, VoIP providers started allowing calls between the two phone systems where the information travels through the network using VoIP until the end where it is transferred into PSTN via a VoIP ↔ PSTN gateway. Hence, VoIP providers can offer phone calls at a lower price and at a long distance. [6] There are other scenarios available e.g. IP ↔ PSTN ↔ IP, PSTN ↔ IP ↔ PSTN and some other variants of these scenarios. [7] But situations rarely require any other setup than those mentioned above.

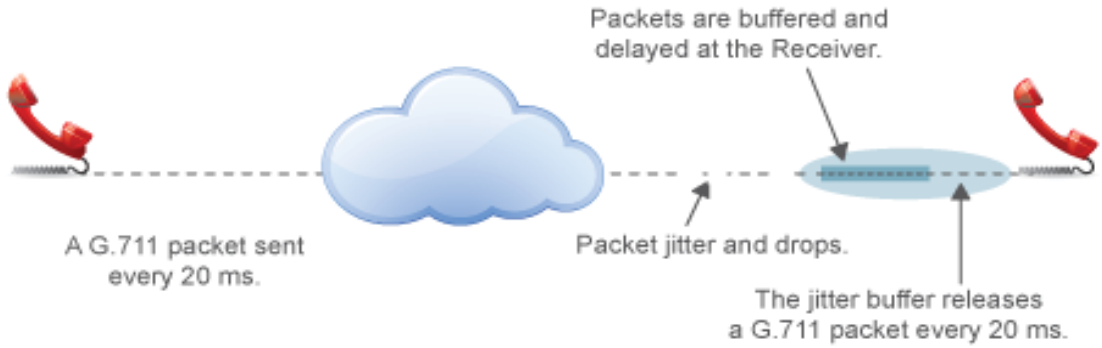

Fig. 1 How VOIP Packets Work

Session Initiation Protocol (SIP)

SIP is a peer-peer signaling protocol for VoIP. It is developed by the IETF MMUSIC Working Group and defined in RFC 2543. [8] It is a proposed standard for following:-

Initiating,

Modifying, and

Terminating an interactive user sessions.

It involves multimedia elements such as video, voice, IMs, online games and virtual reality.

This protocol requires a simple core network with intelligence embedded in endpoints. Therefore, it is highly scalable. [9] It closely resembles HTTP and SMTP and hence SIP sits comfortably alongside Internet applications.

SIP-Allied Protocols

SIP interoperates with:

SDP: To describe the payload of message content and characteristics

SAP: for advertising multimedia session via multicast

RSVP: To reserve network resources for providing QoS

RTP: For real-time transmission

RTSP: for controlling delivery of streaming media

RADIUS: For authentication

LDAP: For location discovery.

Real Time Protocol (RTP)

Multimedia services like audio and video require RTP to communicate. RTP provides the necessary end-to-end conversation requirements for time critical data transmission. RTP and RTCP protocols were designed to run independently over the transport and network layers. [10] RTP often runs in unison with the User Datagram Protocol (UDP). A RTP packet comprises of a sequence number that allows the receiver to rebuild the data that the sender has sent in the apt order.

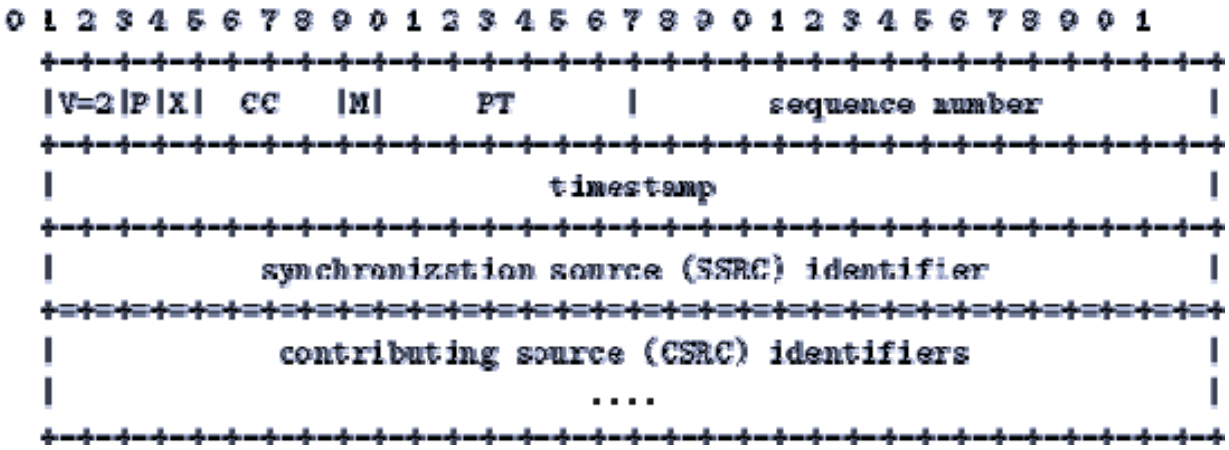

Fig. 2 RTP Packet Format

Codec

A codec, which stands for en-coder and decoder, converts an audio stream into compressed digital stream for transmission over network and vice-a-versa for reply. This is the main concept behind the VoIP. [11] It converts each pulse sample into digitized data and reduces its size using compression algorithm for transmission.

III. ANALYSIS METHOD

VoIP based communication analysis of x-lite VoIP application in wireshark.

Step 1: Open x-lite application

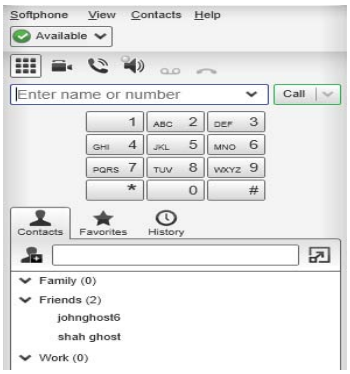

Fig. 3 x-lite Applications

Step 2: Start calling for conversation

Fig. 4 Calling shah ghost

Step 3: Wireshark will start showing the captured SIP packets with calling "shahghost"

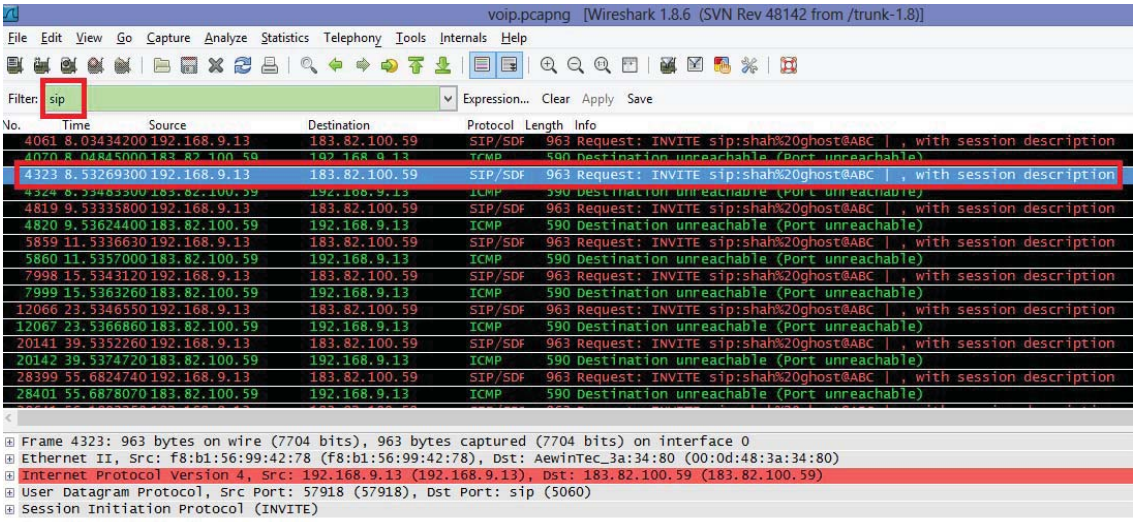

Fig. 5 SIP Protocol Packets

Step 4: To understand SIP packets analysis, select Statistic Flow Graph in the menu bar. This is the resulting flow diagram of the communication.

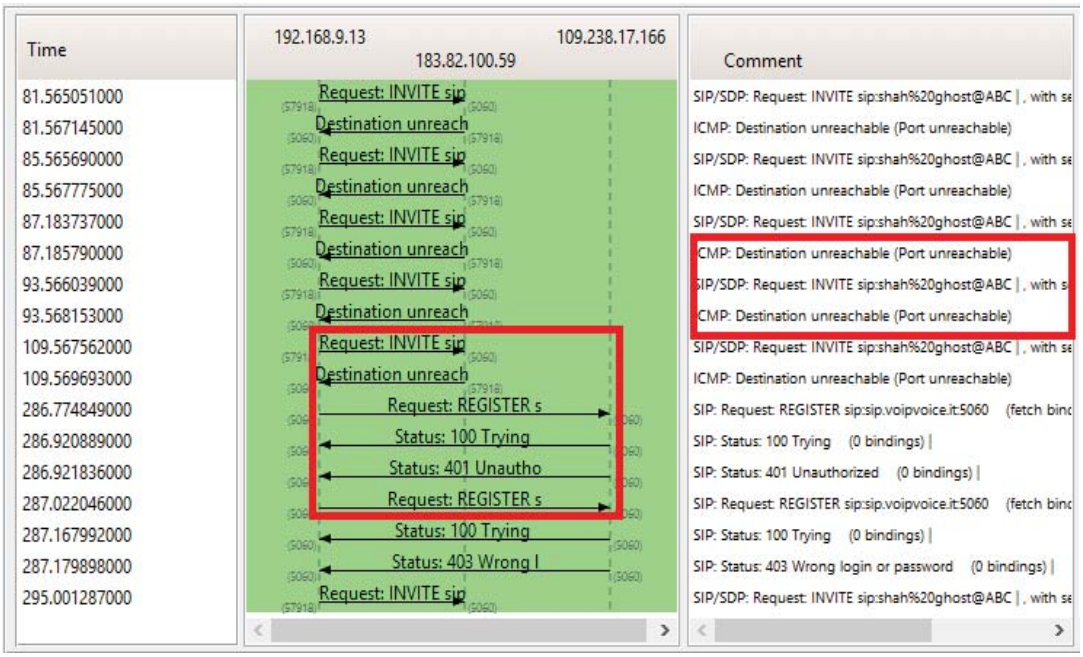

Fig. 6 Graphical View of Conversation

Step 5: The call list or call summary in VoIP bar is shown in this figure

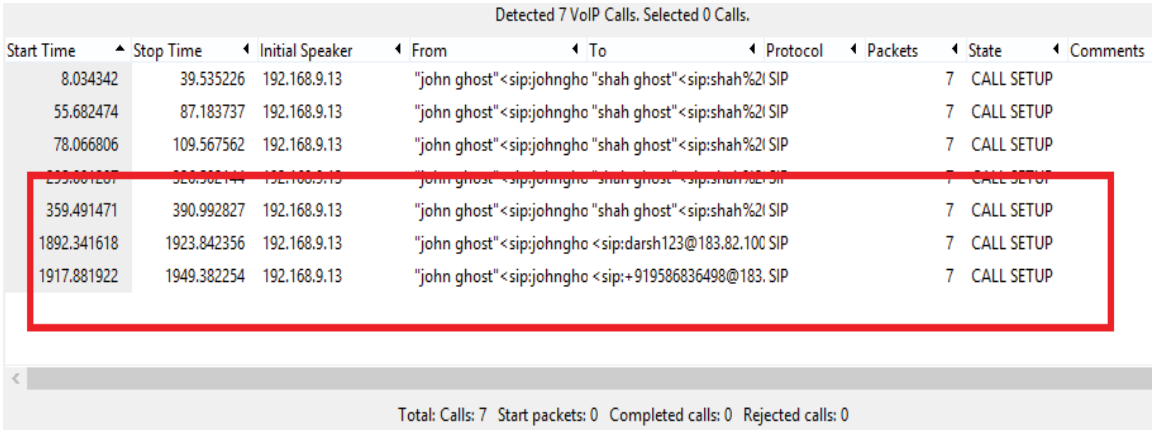

Fig. 7 VoIP Calls Table

Step 6: In the final stage of packet content analysis, mail id of users & application usage for VoIP communication and related IP addresses can be gathered.

Fig. 8 SIP Packet Analysis

IV. RESULTS FROM APPLIED METHOD

The flow diagram gives overview of messages transmitted between the caller and the called. The destination phone does not appear in the graph shown because; there is an intermediate server in between the end users. The packet capture and content inside those packets on the server side are missing.

The caller cannot be viewed from the receiver or client side. All transactions between caller and called can be observed on the intermediate server with NAFT tools. Analysis of log files and packet capture can be done. So, this graph gives the capture of transmitted packets between the source and the SIP server.

192.168.9.13= X-Lite Client

183.82.100.59 = SIP server

The process is further divided into following four parts for understanding complete scenario, Three-way handshake and Authentication process.

Client sending "INVITE" to the server as destination for permitting to talk with the "shah@20ghost@ABC" representing called in this scenario, which can be reached through the domain server named sip16.youroute.net.

Server responds by sending "STATUS" packet with code "100". This is to acknowledge against the INVITE request and state that there is another action that has to be executed first, before calling the destination number. Here in this scenario RADIUS protocol is used for contacting the authentication server.

Server replied a "STATUS" message to the caller with the code "401". The meaning of this is that, the caller has to send its registration information. In fact, first time the server rejects the first call from the caller in order to ask the caller to authenticate first. The "401" response contains the "challenge" for the digest authentication.

Client responds with the request "ACK" message to acknowledge the authorization message received from the connected SIP server which chosen for the first transmission.

V. FUTURE WORK

Automated SIP packet analysis technique can be developed. More sound results can be achieved by monitoring the intermediate servers. Logs can be maintained and analyzed for detecting the VoIP call transmissions.

VI. CONCLUSION

After forensic analysis of all network processes, VOIP analysis is carried out by using Colasoft Capsa, Wireshark and Cascade Pilot software. For the attack, Linux platform is used in which many different types of techniques like Ettercap, SET, Scripts etc. are available. In the output of live detection IP address, MAC address, Packet analysis, conversation between IP & MAC address etc. are found. In the VOIP analysis, conversation & session between two users & analysis of VOIP packet or Graphical view are also found.

REFERENCES

[1] Ahmad Almulhem, (2009) ―Network Forensics: Notions and Challenges, IEEE International Symposium on Signal Processing and Information Technology, pages 463-466, Dec 2009.

[2] François, J, State, R. Engel, T. Festor, O (2010)Digital Forensics in VoIP networks IEEE International Workshop on Information Forensics and Security (WIFS), Vol 1,pp-1-6, Dec 2010

[3] Ibrahim M, Abdullah, M.T. Dehghantanha, A ―VoIP evidence model: A new forensic method for investigating VoIP malicious attacks IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), pp 201-206, June 2012.

[4] Hofbauer, S, Quirchmayr, G., Beckers, K. A Privacy preserving Approach to Call Detail Records Analysis in VoIP Systems IEEE Seventh International Conference on Availability, Reliability and Security (ARES), Aug 2012

[5] Gao Hongtao ―Forensic Method Analysis Involving VoIP Crime IEEE Fourth International Symposium on Knowledge Acquisition and Modeling (KAM), pp 214-243, Oct 2011.

[6] Ahmad Azab,Paul Watters, Robert Layton ―Characterizing Network Traffic for Skype Forensics IEEE Third Workshop (CTC), on Cybercrime and Trustworthy Computing, pp-19-27, Oct 2012

[7] Y.Q. Wang, M. Qi (2011), ―Computer Forensics in Communication Networks, IEEE International Communication Conference on Wireless Mobile and Computing Nov. 2011

[8] Khidir M. Ali (2012), Digital Forensics Best Practices and Managerial Implications, IEEE Fourth International Conference on Computational Intelligence, Communication Systems and Networks,pp-196 – 199, Jul 2012

[9] Edewede Oriwoh, Paul Sant (2013)," The Forensics Edge Management System ", IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 10th International Conference on Autonomic & Trusted Computing, pp-544 - 550 Jun 2013.

[10] Eviyanti Saari, Aman Jantan (2013), "E-Cyborg: The Cybercrime Evidence Finder", 8th IEEE International Conference on Information Technology in Asia (CITA), pp-1 - 6, July 2013.

[11] Manesh T, B Brijith, MahendraPrathap Singh, ―An Improved Approach towards Network Forensic Investigation of HTTP and FTP Protocols, International conference on Advances in Parallel Distributed Computing Communications in Computer and Information Science, Springer Berlin Heidelberg, Volume 203, 2011, pp 385-392.