IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 9, Issue 1 (Jan. - Feb. 2013), PP 61-65
www.iosrjournals.org

A Comprehensive study on tracking VoIP Caller

Hardik Upadhyay[1], Prof. S.D. Panchal[2]
[1]*IT Systems and network Security, Gujarat Technological University, India*
[2]*CE Department, VGEC, Chandkheda, India*

Abstract (11Bold) : *Session Initiation Protocol (SIP) is most extensively usable VoIP protocol which works on application layer. It uses Transmission Control Protocol or User Datagram Protocol which further uses Internetworking Protocol for establishing VoIP communication. None of these protocols including SIP provides absolute location information which provides caller's location in latitude and longitude. Location tracking is an essential feature which must be incorporated to enhance the security and to provide emergency call services. This paper presents basic understanding of SIP and its messages. It also describes few of the generic solutions for location tracking of VoIP and issues related to those solutions.*

Keywords (11Bold) *- VoIP, VoIP caller tracking, Session Initiation Protocol, VoIP caller identification*

I. INTRODUCTION

Internet has no boundaries. Skype, Google Talk, Yahoo voice /video etc. are all applications that enable the use of the Internet for voice and video conversations. But these all are proprietary, and needs to have same software application on other end in order to established audio/video call. These propriety applications are more secure as they are passing all the information in encrypted format and optimization of protocols has been done nicely. But there is less scope for any modification in existing one. But true VoIP system does not require being dependable on single application. [1]

Session Initiation Protocol (SIP) works on application layer and it is a text based signalling protocol. It is mostly used protocol in VoIP. It is text based protocol like HTTP. All SIP supported systems would able to established audio/video communication without having specific device or software. Just SIP supported software or hardware is needed. Many SIP User Agents (UA)/SIP clients are available in the form of soft phone, IP Audio phone, and Video IP phone. Now a day's smart phones also compatible to the SIP, so that we can even use our mobile phone in order to use VoIP services. We just need to connect them into the network/Internet. However, basic protocol for communication is Internetworking Protocol (IP). So this technology is known as VoIP (Voice/video over IP). It offers cost effective, flexible and scalable solutions, and due to these reason many new VoIP applications are coming into existence. [2]

However, all forms of communications and original location of caller need to be monitored for security purposes to ensure their correct usage. With the development of more and more VoIP applications, monitoring and tracing of these applications is becoming a more difficult task. It is also difficult to provide emergency services (like 911 in us) using VoIP, as it is also requires identifying caller location. [3,4]

Monitoring on ongoing communication can be achieved by lawful interception from server side, but most of the detection techniques are based on standard protocol and IP address identification. IP address doesn't provide actual location of caller; specifically in the form of latitude and longitude, and IP address may be spoofed, however it is not going to established the call in case of spoofed IP address. User may trick the server by using anonymous proxy servers. In that case server will have wrong IP address information. This paper presents generic techniques for detection of actual location of caller in public network. It also contains the proposed method that would be ideal for live tracking of SIP caller. Other associated terms with VoIP are IP telephony, Broadband telephony. [5]

Section II describes Session Initiation Protocol and its functionality. It also describes how IP telephony works using SIP by explaining various messages of Session initiation Protocol which are important to establish VoIP call. Section III contains explanation of related work and issues associated with them.

II. OVERVIEW OF SIP

Session Initiation Protocol (SIP) is an application layer protocol which provides session management between VoIP client and server. All SIP supported application can communicate to each other, so it is broadly usable VoIP protocol. [6]

SIP supports basically five services for managing communication: [7]

User location: It will determine end device which will used in communication
User availability: Identify if the end system is available for communication
User capabilities: It defines media to be used for communication

Session setup: Established session for communication and manage it.

Session management: It manages session in terms of modification, transfer and termination.

SIP basically works on client-server mechanism, which uses request and response method just like Internet applications. Addressing method is also similar as e-mail which will identify user uniquely. Normal SIP URI would appear like follows:

- sip:1111@company.com
- sip:1112@10.1.1.1

SIP uses either DNS or IP for locating user. SIP messages can also have other information like authentication tokens, session identifier and Session Description Protocol (SDP). SDP is used to exchange session capabilities and features which will works along with SIP. [6,12]

A. Components of SIP [6]

User Agent Client: Actual client who is requesting for call to establish, it is also known as Terminal Equipment. Eg: Soft phone, IP phone, SIP enabled smart phone

User Agent Server: It is a server which is responsible to initiate the call to the destination. It is the actual server who is going to provide VoIP services.

Registration Server: In order to establish call, TE(Terminal Equipment) user has to get register to the SIP server. So registration server will performs the authorization of user.

Proxy Server: It works as a forwarder, in which UA will locate one proxy server, proxy will forward it to another and so on up to the destination server. It also provides routing, authentication, authorization, address resolution, and loop detection.

To set up entire VoIP infrastructure, all of above components work together.SIP servers can also works with other application or servers like RADIUS to provide services, such as authentication or billing.

B. SIP Messages [6, 7]

In order to understand how IP telephony works , one needs to understand SIP messages, and how it works to establish the communication. As SIP is the protocol responsible to initiate the call. SIP defines lots of messages, but to make proper communication followings are the essentials.

As discussed SIP messages are either request type or responses type. Response would a reply to the request message; the main messages that can also known as methods describes as follows:

- REGISTER- User Agent Client (UAC) will send this message for registration to the server. In order to established communication user has to perform registration. Server will validate UACs identity.
- INVITE— UAC will send this message to initiate call or conference, which server will forward to another UAC.
- ACK— Server and UA will send acknowledgement messages in the response of receiving various messages like INVITE.
- CANCEL—It ends the session of call which is not fully established.
- OPTIONS—It contains various fields, which contains response of queries mainly the values contains capabilities of a server.
- BYE—Normal termination of fully established call.
-

III. RELATED WORK

This section describes the solutions for location identification of VoIP caller. This section also describes the issues associated with the explained solutions

GEO Track

This method uses traceroute mechanism to identify location of VoIP caller. After determining the path, the location will be inferred from the DNS names of router interfaces and the location of the last router is assumed to be estimate of the target host's location. [8, 9]

Observations:

- The accuracy of this method depends mainly on how accurate the DNS records are.
- The traceroute result will also affect the location deduced from this method and this cannot be guaranteed to reflect the actual location of the target host, as user may use anonymous proxy server in order to establish call.
- If user is using mobile broadband, than this method would not give accurate location information.

Database Approach

This solution describe that identification of VoIP caller location can be done by identifying location of end device and port where device is connected. So, by presuming the location of the endpoint device is stored in the database, a general location of the *VoIP* phone could be determined by knowing where the network device is located. [10]

Observations:

- Network devices are frequently upgraded or replaced, and they are generally kept in a rack in a communications "closet". So in case of device with which VoIP phone is connected, is replaced or changed, then we have to upgrade all information into database manually. In case of deice located in datacenter, it seems to be closest, so it is difficult to distinguish the location.
- There might be one or fewer such closets on each floor of a corporate building, and so keeping a database of the network devices and their port locations is prone to human error
- Useful in wired connection only, in the case of wireless connectivity, it is quite impossible to provide generic solution, so that end device transfer the location information along with call.

RFID Tag

This solution provides the location information for providing emergency call services. This solution comprising reading RFID tag data from at least one RFID tag using an RFID reader operatively associated with the VOIP terminal; and determining the VOIP terminal location based on RFID tag data. [10]

Observations:

- No Global standard for RFID, So it is difficult to implement globally.
- Illegal tracking can be done on RFID tag; If attacker fetch the RFID of the device, than it is very easy for attacker to track the device.
- RFID tags could be read from a distance without the owner's knowledge, leading to the disclosing of location or other sensitive information contained in the RFID tag's memory
- As it is possible to clone RFID tag, it may be used to fool the authority. So it is a major security concern.
- RFID tag can work up to certain distance, so mainly useful in the application like shopping mall, so in order to get location information in public network, is difficult.

On demand database approach

This solution was implemented for determining the location of a VoIP caller includes receiving an emergency call from a VoIP phone from the internet via a VoIP enabling device. A device identifier of the VoIP enabling device through which the call from the VoIP device originated is received. The device identifier is compared against a pre-defined table of device identifiers, where each device identifier in the table has an associated physical location. The physical location of the VoIP enabling device is returned during the call from the VoIP phone.

In this solution, the user who wants to use emergency services, which require location information of caller, need to get registered to the provider in prior. [10]

Observations:

- Static entry in database, so can not consider as a reasonable solution. It has to be dynamic in nature.
- If user moves from one location to while call is going on, this method is not effective. So no live tracking is provided.
- User has to prior register himself in order to use emergency service .

GPS integration with VoIP Device

In this solution GPS device had been integrated with VoIP device. So when user dials emergency call, it passes the location information with INVITE packet. It can be consider one of the finest solution in order to identify user location in public network. [10,11]

Observations:

- As it is passing location information in INVITE packet, it can pass location at the time of call establishment, but if user moves after establishing call, than it is possible to get location information in this solution. So no live tracking can be done using this solution.
- Only useful for Emergency services up to certain extent.

- GPS tracking information, although relatively accurate, still has an uncertainty window around it of about 15-30 feet
- More power consumption
- GPS may not properly works in to internal areas of buildings
- It would not provide floor information in case of multi story building

GEO Cluster

With this technique, IP addresses which correspond to the co-located hosts are grouped together. IP-to-location mapping information is then used to infer geographical location of the cluster. The address prefixes contained in BGP routing tables are then used to infer the location of the cluster. Given a target IP address, at first the geographic cluster to which it belongs is determined, and then an estimation of its location will be calculated to be that of the geographic cluster. So, the physical location of the cluster is assumed as user's location. [10,11]

Observations:

- The accuracy of this method also depends mainly on accurate mapping information being available
- It will not work in case of caller is using anonymous proxy server
- Would take more time to get location information, so not proper solution for deplying emergency call services

DHCP lookup

Dynamic Host Configuration Protocol (DHCP) servers have additional configuration options that allow them to store more information for each client than just the IP address. This information can include: the subnet mask, the domain name, the router IP address, static routes and physical location information. The SIP proxy server can also obtain the location information of a User Agent (UA) by querying DHCP server. The DHCP database must be updated with this additional information. [11]

Observations:

- Static entries are needed for location information for each IP address corresponding to MAC address.
- This will not work on Static IP address, as in internet scenario, one can have static IP address.
- Cannot provide accurate location information in terms of latitude and longitude

WHO IS lookup

Whois service provides the information about the organization and the person who has registered the site. It contains information such as: telephone numbers and mailing addresses. Based on this information, the physical location of hosts can be determined. [12]

Observations:

- The main concern with this method is that all of the hosts may not be located at, or near, the addresses of the registered organizations.
- Additionally, whois database data is provided manually, so incorrect or false data may be submitted. Furthermore, data must been updated periodically in order to be reliable.

Tracking VoIP Call using Digital Watermarking

This solution basically focuses on lawful interception of peer to peer VoIP call. Generally a VoIP packet passes through many peers in internet scenarios before reaching to their destination. So it is difficult to determine who is talking to whom. [13]

This solution presented watermarking technique, in which digital watermark would be embedded with VoIP signalling and media packets, which would help the law agencies to intercept VoIP call. This scheme is also known as packet marking scheme. [13]

Observations:

- This technique does not have global monitoring technique.
- It focus on finding out if some parties in which law agencies are interested to find out and intercept if have communicated.
- It does not provide absolute location information of caller, so cannot be useful to identify originating location of caller.

IV. CONCLUSION

None of the solution is passing location information in terms of latitude longitude except one solution, which was only useful for emergency call services which are integrated with PSTN. So for enhancing the security in terms of location identification, it is not that useful

In internet scenario, server needs to fetch exact location information in order to enhance security, and to provide live tracking functionality. Some Ideal Solution should be provided to provide location information in the context of security. It should provide accurate location information on the fly (live tracking should be possible) .It should provide location information even in the case if someone is using the anonymous proxy server to established the call. Device should not allow establishing call if it is not passing location information and location spoofing should not be allowed.

Acknowledgements

Apart from the efforts of me, the success of any task depends largely on the encouragement and guidelines of many others. I take this opportunity to express my gratitude to the people who have been instrumental in the successful completion of this work. I would like to express my deepest gratitude to Prof. S.D. Panchal, HOD IT, VGEC, Chandkheda, Ahmedabad, Gujarat. I can't say thank you enough for his tremendous support and help. I feel motivated and encouraged every time I attend his meeting. I take immense pleasure in thanking Mr. Naresh Kumar Gardas, course coordinator, C-DAC and Ms. Kiran Bhagiya, Coordinator, GTU for having permitted me to carry out this work and for all valuable assistance in this work.

REFERENCES

[1] Rakesh Arora,1999, VoIP protocols[online]. Available: http://www.cis.ohio state.edu/~jain/cis788-99/voip_protocols/index.html
[2] Hsien-Ming Hsu a, Yeali S. Sun a, Meng Chang Chen, Collaborative scheme for VoIP trace back, Science Direct, 2011
[3] Ram D, Sonia F, Henning S, Joao C, Issue and challenges in securing VoIP , Science Direct, 2009
[4] Zourzouvillys, T.; Rescorla, E., An Introduction to Standards-Based VoIP: SIP, RTP, and Friends, 2010,IEEE international conference, Page(s): 69 - 73
[5] Ashtarifar, S.; Matrawy, A, Determining Host Location on the Internet: The Case of VoIP Emergency Calls, Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference, , Page(s) 1-5,2009.
[6] Rakesh Arora,1999, VoIP protocols[online]. Available: http://www.cis.ohio state.edu/~jain/cis788-99/voip_protocols/index.html
[7] J. Rosenberg,H. Schulzrinne,G. Camarillo,A. Johnston, J. Peterson,R. Sparks, (June 2002)SIP: Session Initiation Protocol[Online]. Available: http://www.ietf.org/rfc/rfc3261.txt
[8] Jose c, Haitao T, Enhancing SIP with Spatial Location for Emergency Call Services, 2002, IEEE international conference, Page(s): 326 – 333
[9] V. Padamanabban and L. Subramanian, Determining the geographic location of Internet hosts, ACM SIGMETRICS Performance Evaluation Review, vol. 29, no. 1, pp. 324–325, 2001
[10] David S. Benco, Sanjeev Mahajan, Baoling S. Sheen, Sandra Lynn True, 2008, Methods and apparatus for improved 911 support for VoIP service , US patent US0242660 A1
[11] Dennis J. Hasenfang, Christopher C Willis, Apr 26, 2011, Emergency services for voice over IP telephony, US patent US7933580
[12] Ram D, Sonia F, Henning S, Joao C, Issue and challenges in securing VoIP, Science Direct, 2009
[13] X.Wang, S. Chen, and S. Jajodia, Tracking anonymous peer-to- peer voip calls on the internet *ACM Conference on Computer and Communications Security (CCS)*, 2005
[14] C. Holmberg, Ericsson (April 2011) Indication of support for keep alive with SIP [Online]. Available: http://tools.ietf.org/html/rfc6223