Security Issues of SIP based VoIP System

Arpita Gautam
Department of information and technology
RKGITW
Ghaziabad, India
arpitagautam@gmail.com

Manpreet Kaur
Department of information and technology
RKGITW
Ghaziabad, India
manprit.kaur007@gmail.com

Rahul Sharma
Department of information and technology
RKGITW
Ghaziabad, India
rahul.gla@gmail.com

***Abstract*- In this booming world of internet, telephone traffic is just another application running over it. Voice over Internet Protocol, also known as VoIP, is a technology used for transferring voice information using the Internet Protocol. The nature of packet network used by VoIP in general is that the data that has to be transmitted is split into small packets that include small amount of address information added to each packet. This form of transmission is conceptually superior to conventional circuit switched communication in many ways. VoIP has made the voice traffic somewhat more efficient and cost less however a plethora of security issues are associated with VOIP technology. In order to effectively secure a VoIP network, efforts are involved significantly. This paper provides a brief description of VoIP highlighting its issues. Firstly, the paper discusses the issues that may occur while transferring voice data over internet. Secondly, the paper discusses about the session initiation protocol (SIP) architecture and its issues since adoption of SIP based telephony risks to system confidentiality, integrity and availability. Finally the paper explains some solutions to SIP based attacks and conclusion.**

Index terms—VoIP, SIP, Security Issues, and Solution to VoIP Issues.

I. INTRODUCTION

VoIP - The transmission of voice over packet-switched IP network is one of the most important emerging trends in telecommunications. VoIP is subject to many security issues which are uniquely applied to both telephony and traditional Internet data transmission. The differences in their architectures result in significant security issues. The primary tools used for security purposes are protocol analyzers, vulnerability assessment utilities and security monitoring utilities. These tools have reached a higher level of satisfaction for protecting network protocols, operating systems and other applications from attackers. The two prominent features of VOIP are greater flexibility and lower cost for the enterprise, but VOIP should not be installed without careful consideration of the terms and conditions for security issues introduced. VOIP security issues can be resolved just as other security issues are resolved. Although the security tools for developed technologies are efficient, still it is difficult to develop strong security tools in the early stages of an emerging technology such as Voice over Internet Protocol (VOIP).

II. Is VoIP REALLY A MAJOR PROBLEM?

No, it's not. It is just interpreted in such a way because it is a bit different problem. Since a lot of manual verification is involved with telephony so there are chances that vulnerabilities may go unnoticed with the recent VOIP assessment tools. There are millions of techniques for identifying the threats but yet sometimes there are few issues that cannot be identified by database and web application scanners. And this is not a major problem to be worried about.

III. ISSUES OF VoIP

A. Toll Fraud

It is one of the most threatening issues for most of the large organizations. It is a kind of treat that most of the time go unnoticed allowing the attackers to rack up a large bill at the organization expense. These kind of attacks are difficult to identify as they are very time consuming and inconvenient to scan them. Toll frauds are very easy to execute. Just a small error in configuration for dial plan, and fraud is done. Attackers can remotely access the lines which were left open for test purposes. It is very beneficial from the attacker's point of view because no real costs are involved once the toll fraud is accomplished; the attacker can also abuse the services quiet quickly, for example by reselling it.

B. Eavesdropping

In VoIP, eavesdropping is an attack that allows the intruder (unauthorized person) to listen and record private

ISBN: 9788175157538

phone conversations. It is a passive attack that intercepts and reads the messages and conversations by unintended party. Eavesdropping is not a particular problem of VoIP services instead it is a very common problem in communication services. Here we are highlighting this problem because of the following reasons-

Firstly, VoIP calls are not encrypted in general; there are plenty of encryption options available but no such appropriate algorithm can be implemented due to the fragmented nature of VoIP. There's no simple solution to ensure end to end encryption, with end points as diverse as traditional telephones. Secondly, eavesdropping can lead to unexpected consequences because people may use telephonic system for sharing their important and private information such as Credit Card numbers, Social Security numbers or any other confidential information. Eavesdropping can also cause unauthorized access to confidential business data in a company. Despite of being a very common problem, eavesdropping is a very destructive threat in VoIP.

C. Caller ID Spoofing

A spoofing attack is an attack in which a person can masquerade being the one, which actually he is not. Caller ID spoofing doesn't require any technical knowledge and hence has become very easy to be accomplished. Spoofing was practiced even before the popularity of VoIP but with VoIP however it became a lot easier to be done anonymously. Spoofing is now decades old but the general public is still not aware about it.

D. Call Hijack

Call hijack is the attack in which one of the end points of conversation is exchanged with the intruder, in VoIP and classical telephony. The consequences of call hijack attack are very similar to eavesdropping attack such as access to confidential data. Generally if the attacker is successful in conducting a call hijack then to avoid raising suspicions he evolves it into man in the middle attack.

E. DOS (Denial of Service)

Also k/as DOS is an attack on computer system or network which may lead to loss of network connection and services by consuming the bandwidth or overloading the network resources of the victim's system.

A DoS attack can be perpetrated in a number of ways.

(1) Blocking of resources, such as bandwidth, disk space, or CPU time.
(2) Interception of configuration information, such as routing information.
(3) Disruption of physical network components.

F. Man in the Middle attack

Man in the middle attack (MITM) is a passive attack where an attacker is able to analyse, insert and modify the messages send between two parties without either party knowing that their private information has been compromised. The attacker is able to observe and intercept messages going between the sender and receiver. MITM attack can be used for conducting other sub attacks such as eavesdropping and Denial of service attack.

IV. SIP

SIP is the Internet Engineering Task Force (IETF) protocol that initiates sessions for a two-way communication. It is important to note that sip can be used in any session driven application or technology and is not particularly used in VoIP only. SIP is similar to HTTP, is text based and can be carried by UDP, TCP and SCTP. UDP can be used to increase speed as well as efficiency and decrease overheads, and TCP can be used if SSL is incorporated for security services. SIP uses one network port with 5060 as the default value.

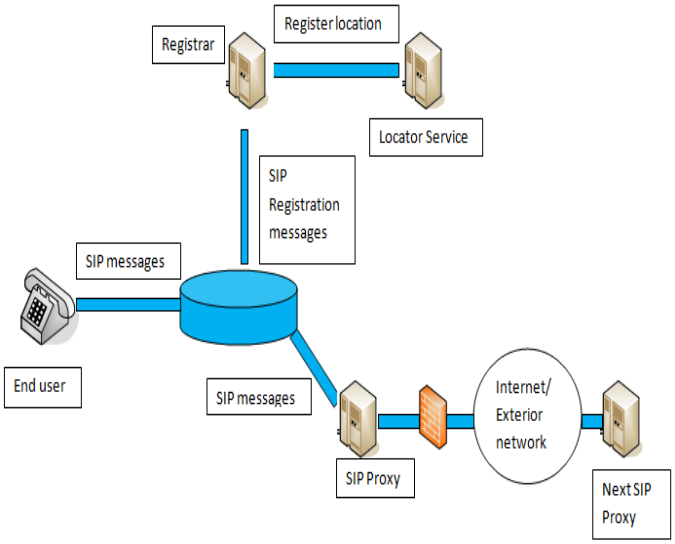

Fig: 1 SIP based VoIP architecture

A SIP network is made up of end points (terminals), registrar (to register location information), location server (for locating users) and a redirect server or a proxy server (for end to end message transmission). Both the location server and the registrar may be integrated in the proxy server.

ISBN: 9788175157538

V. SIP BASED SECURITY ISSUE

A. *SIP Based DOS*

a) SIP bombing

SIP bombing is an attack that includes the transmission of a huge quantity of forged SIP messages to a targeted VoIP system and these SIP messages will require the allocation of computational resources for interpreting and decoding them. While the system is busy decoding the forged messages, valid ones will be decoded at a much slower rate and therefore the overall performance of VoIP conversation will doom down. When subjected to heavy SIP traffic hardware IP phones have crashed and even some applications of softphones have also crashed and became unresponsive or unusable. SIP Bombing has been successfully tested on VoIP devices.

b) Cancel or Bye DoS

Two different malicious actions are reunited under the same category because the attack blueprint is the similar for all the cases: an attacker sends a crafted SIP message to a receiver (victim) after detecting that the receiver (victim) has established a SIP session/VoIP conversation with another user. For launching an effective SIP-CANCEL attack, it has to be done in the time window available between the sending of the INVITE method and the receiving of the last ACK that ends the SIP session initiation handshake. Doing so will leave a very restrictive window to the hacker. On the other hand SIP-BYE can be launched at any moment after a VoIP conversation has started. The attack window available which is the entire duration conversation makes a successful attack to be realized easily.

B. *SIP based Man in the Middle/Call Hijacking*

Since both the attacks have the similar consequences and similar attack blueprints, here they are treated as a single entity. When a call is hijacked successfully, it becomes very easy to forward it to the original caller, thus realizing a MITM attack. Two major types of SIP based MITM attacks can be distinguished as:

a) Manipulation of the Registration Records

In this type of attack, an attacker can receive all the victim's calls by manipulating the registration that is associated with the victims SIP URI on the same network. The identity of a UA is accessed by registrar. The "From" header of a SIP request can be changed and hence open to malicious registration. Further, the UDP protocol can be spoofed very easily which are used for registration requests since they are connectionless and SIP registrars are not required to authenticate the UA requesting a registration. When authentication is used for security purpose, it is not that strong, and only involves use of a MD5 digest of the username, password, and timestamp-based nonce sent in the authentication challenge. Extreme cases of such attacks include exterior attackers that are able to successfully register as internal users to the SIP registrar, although this situation is highly improbable.

b) 3XX Response codes

The 3xx SIP response codes class corresponds to provide information to the requester that the specific actions has to be undertaken in order to successfully accomplish the request. The 3xx response codes class of SIP based attacks relies on forged responses. The attacker has following outline:

- The victim issues a SIP request (an INVITE request for example)
- The attacker then sends a 3xx code response to the initiator. The attackers misuse the identity of either the caller UA or one of the SIP components (proxy, registrar etc.)
- The victim's SIP client receives the forged 3xx response and redirects its communication through the attackers system for the rest of its request; the attack is complete.

The simplest attack of this type is the Call Hijacking attack. In this scenario, the attacker upon detecting that the victim has issued an INVITE Request sends him a response. The victim in turn contacts the attacker for achieving the SIP connection. The attacker is not restricted to UAs when choosing his forged identity. By careful manipulation of 3xx responses and by spoofing a proxy server, a variant of the above attack can be achieved with the Proxy response code.

Similar to SIP DoS attacks; it's hard to conduct the MITM attacks in real-live scenarios due to the mitigating factors:

- Like SIP based DoS attacks these attacks are also opportunity based attacks.
- Headers reproduction: for successful implementation of MITM attacks, it require that the forged responses coming from the attacker machines contains the right header content to be accepted as legitimate, similar to SIP DoS manner
- Authentication mechanisms: Strong authentication mechanisms involving secured feature

ISBN: 9788175157538

for the registration process diminish the chances of registration hijacking.

VI. SOLUTIONS TO SIP BASED ATTACK

So far, we have discussed a number of significant concerns with VOIP. All the attacks concern to VoIP rely on tampering and creating spoofed SIP messages. However, many of the problems are solvable. Despite the difficulty associated with these solutions it is well worth to provide a solution for avoiding the attacks such as protecting SIP content from tampering, interception, and reply with strong encryption and authentication mechanisms.

A. TLS usage within SIP

IPsec can be used to provide authentication, integrity and confidentiality for the transmitted data and supports end-to-end as well as hop-by-hop encryption. IPsec is used to provide encryption for SIP messages at the network layer. This type of security is most suited for securing SIP hosts in a SIP VPN scenario (SIP user agents/proxies). IPsec works for all UDP, TCP and SCTP based SIP signaling. One accepted protocol for key management is Internet Key Exchange (IKE). The IKE protocol provides automated cryptographic key exchange and management mechanisms for IPsec.

B. IPsec usage within SIP

IPsec can be used to provide authentication, integrity and confidentiality for the transmitted data and supports end-to-end as well as hop-by-hop encryption. IPsec is used to provide encryption for SIP messages at the network layer. This type of security is most suited for securing SIP hosts in a SIP VPN scenario (SIP user agents/proxies). IPsec works for all UDP, TCP and SCTP based SIP signaling. One accepted protocol for key management is Internet Key Exchange (IKE). The IKE protocol provides automated cryptographic key exchange and management mechanisms for IPsec.

VII. CONCLUSION

After conducting this VoIP Security Study we can conclude that VoIP security is in an incipient phase at the moment. Threats and attacks can be defined and theorized, but are difficult to carry out in practice, mainly due to the lack of knowledge and testing opportunities for attackers. However, as soon as VoIP networks will gain more popularity, attackers will probably become very interested in this new technology. The solutions chosen for the VoIP threats analysis shapes an audit guideline, underlines solutions for combating VoIP threats.

VIII. ACKNOWLEGMENT

A research work owes its success from commencement to completion, to the people in love with researchers at various stages. Let us in this page express our gratitude to all those who helped us in various stage of this study. First, we would like to express our sincere gratitude indebtedness ***to*** **Mrs. Kadambri Agarwal** (HOD, Department of Computer Science and Engineering/Information Technology of RKGITW) for allowing us to work on the topic "**Security issues of SIP based VoIP system**".

We are also thankful to all faculty members of Department of IT, for their true help, inspiration and for helping us in preparation of the final research paper.

IX. REFERENCES

[1] Andrew S. Tanenbaum " Computer Networks," Byblos Bucharest, 2004

[2] Andrew S. Tanenbaum " Modern Operating Systems," Byblos Bucharest, 2004

[3] W.C. Hardy, "VOIP Service Quality: Measuring and Evaluating Packet-Switched Voice," McGraw-Hill, 2003.

[4] Amarandei Stavila Mihai, "Voice over IP security – A Layered Approach".

[5] Răzvan Beuran," On VoIP over Wireless LAN Survey," April 20, 2006.

ISBN: 9788175157538