Analysis Of SIP Authentication In VoIP

Riddhi Patel[1],
Computer Engineering, Gujarat Technological University, India.

Pushkar Jha[2]
Computer Engineering, Gujarat Technological University, India.

Aditya K. Sinha[3]
Principal Technical Officer, CDAC-ACTS, Pune, India.

Abstract

One of the most common ways, where anyone can communicate with each other very easily, and instantly, is, of course, the voice exchange. Public Switched Telephone Networks (PSTN), and Voice over Internet Protocol (VoIP) are common ways of transferring voice communications by using telephone network. These two ways have their own strengths and weaknesses. But as world is moving more advanced technologies at cheaper options, which also, giving rise to threats involved at the same rate.

Although the invention of Voice over Internet Protocol (VoIP) in communication technology created significant attractive services for its users, it also brings new security threats. Finding digital evidence in VoIP malicious attacks is the most difficult task, due to its associated features with converged network. The main goal of this research is the discussion of security issues of SIP, which serves as a signalling protocol for VoIP services. This work especially concentrates on the security risks of SIP Authentication proposed for VoIP forensic analysis. VoIP spoofing is being a common and most important threat to the VoIP users. Attackers and spammers equently spoof identities in order to be untraceable It is technically possible for an attacker to masquerade as another VoIP caller (VoIP spoofing).none of protocols used in VoIP including SIP provide solution for avoid spoofing . This paper presents basic understanding of SIP and its messages. It also describes few of the generic solutions.

For avoiding spoofing and issues related to those solutions. A design of SIP which will prevent VoIP spoofing using PKI concepts and forensic analysis, all this will help in the detection of the spoofing or the fake caller address.

Keywords: *VoIP, Session Initiation Protocol, cryptography, spoofing, Public key Infrastructure, Digital certificate.*

1. Introduction

Internet telephony is becoming more and more important. Gtalk, yahoo, Skype a software, a boom in internet telephony, which was only released in 2004 and has now up to 6 million users being online at any time. The so called Voice over IP (short: VoIP) technology offers cheap calls all over the world. VoIP systems are an attractive alternative compared to traditional telephony for various reasons: use of existing internet infrastructure, cheap connections, no need for expensive hardware, and so on. Recently, with the extensive application of VoIP, the studies of its security problem become more and more important. So, we should strengthen the research on the VolP Network Security and combine it with the characteristics of VolP to push this technology to the next stage, and the digital evidence forensics will become much more important. We can integrate VoIP with IPv6 technology so VoIP is Next Generation Network for communication and its demand is increase over time as call rate is becoming costly. *Today, with the move to SIP trunks and* VoIP technology, spoofing caller ID *is fairly trivial.* Investigators say that the nature of VoIP calls make it difficult to trace the identity or location of the callers. The most outstanding phenomena is Dialling telephone numbers directly by the arbitrary number modification software, for fraudulent activities which is termed as CALLER ID SPOOFING. The internet protocol addresses of persons who use VoIP networks are dynamically assigned, which means it constantly changes so finding the source address is most difficult task after attack. Existing protocol will not provide the mechanism for spoofing detection and prevention. From where actually the call is initialized so that detecting and preventing from spoofing is a challenge in VoIP. It’s very difficult to identify the caller is legitimate one or not.[1,9]

2. Literature Survey

2.1.What is VoIP?[1]

A VoIP stands for – Voice over Internet Protocol (VoIP). Transmission of voice over Internet. In layman's terms VoIP is the transmission of voice over the digital network.

2.2. SIP Overview[2,10]

"SIP is an application-layer control protocol that can establish, modify, and terminate multimedia sessions (conferences) such as Internet telephony calls. SIP can also invite participants to already existing sessions, such as multicast conferences. Media can be added to (and removed from) an existing session. SIP RFC is RFC 3261. SIP is a component of a complete multimedia architecture, and relies on other Internet Engineering Task Force (IETF) protocols. The key to SIP is that it provides only five functions: user location, user availability, user capabilities, session setup, and session management. That is all SIP does. That being said, SIP is flexible and open enough to allow developers to build their own "hooks" into SIP. This flexibility has given SIP an advantage over other "telecommunications protocols," and is why many enterprises are eager to develop, implement, and use SIP.

SIP services for managing communication:

User Location: It will determine the end system to be used for communication.
User Availability: It determine of the willingness of the called party to engage in communications
User Capabilities: It determines media to be used
Call Setup: ringing and establishing call parameters at both called and calling party
Call handling: the transfer and termination of calls

2.2.1. Components of SIP [3].

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

2.2.2. SIP Messages[4,5,6]. 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.

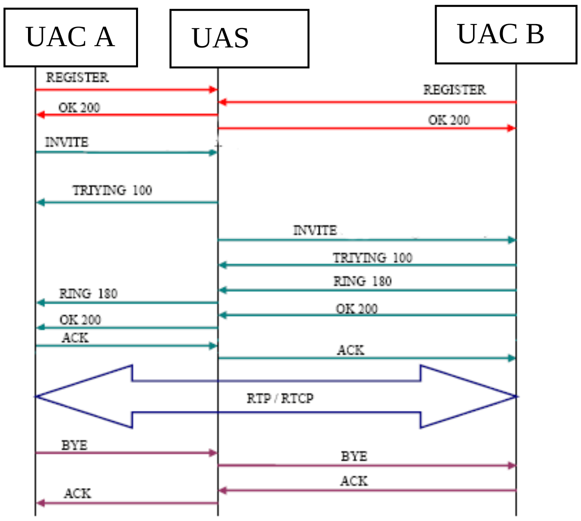

Figure 1. Sequential Diagram of working of SIP between two different User

2.3. VoIP Spoofing

Call spoofing refers to being able to call an extension with a fake identification. Whenever a client calls another extension there is an INVITE packets that is sent to the client which contains the username and the other details of the calling extension. However manipulation of this single packet and sending it to a registered SIP device can result into a call being spoofed. Following is the capture of the invite packet. It may be observed in the following packet that the attribute "from" contains the required data and can be tampered to spoof a call. Or to fake it origin.
For this any one can use a tool that is called as INVITE flood[9].

2.3.1 Why people are doing spoofing[8]

Caller ID spoofing can be used for legitimate reasons; below are a few examples.

1. Business people often use Caller ID spoofing to reveal their business number, on the recipients Caller ID display, should they be calling from outside the business premises, for instance, calling from a mobile phone.
2. Caller ID spoofing is also used to defeat popular telephone services such as "*57 Call Trace", "*69 Last Call Return", "Anonymous Call Rejection" and "Detailed Billing".
3. Doctors use Caller ID spoofing when calling patients from their personal phones, instead of their personal numbers appearing their office number appears.
4. On Skype users are able to assign a Caller ID number in order to prevent their Skype-Out calls from being screened by the person being called.
5. Collection agencies, private investigators and the like use Caller ID spoofing for pretext calls.

And of course many people have used Caller ID spoofing to make prank calls. Then there are the criminal uses of it. Just last month there was a case where customers of Langley Federal Credit Union in the US received calls, apparently from their bank, asking them to call a different number to verify their banking details, card Pin numbers and pass words. Customers where unsuspecting as the calls came complete with the bank's caller ID number. Unfortunately credit union officials confirmed that many customers fell for the scam.

2.4. Issues and Challenges with Existing Approaches

Source IP can not be determine at the time of SIP Authentication as VoIP assign IP address Dynamically. And if it is authorized user then it won't create any problem but if the user is attacker and he wants to attack by doing spoofed call then one can never determine that who has done attack and from where it has been initiated. For that Authentication mechanism should be strong.

3. Related Work

This section describes the solutions for detecting fack call(or spoofed call) from VoIP caller. This section also describes the issues associated with the explained solutions.

- VoIP Spoofing is the most common attack and detecting VoIP spoofing is one of the biggest challenge.
- So my proposed solution for detecting and preventing spoofing is, modify the SIP protocol using Inter domain communication Mechanism.
- In this mechanism I will integrate concept of PKI at the time of SIP Protocol Authentication.
- A PKI (Public Key Infrastructure) enables users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority. The public key infrastructure provides for a digital certificate that can identify an individual or an organization and directory services that can store and, when necessary, revoke the certificates.[7]
- Working of Proposed SIP Protocol

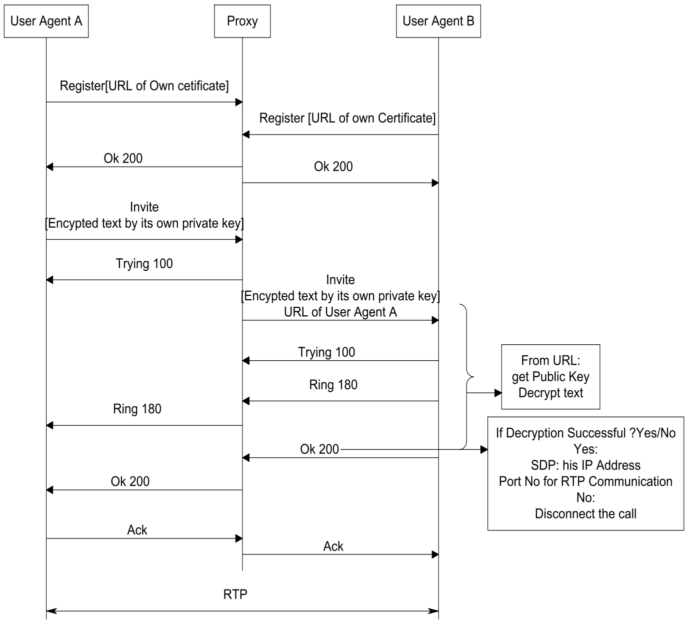

Figure 2. Proposed SIP Protocol

3.1. Advantages and Disadvantages of Proposed Solution

- Effective in avoiding and preventing spoofing
- It will be time consuming in order to get the certificate and public-private key encryption and decryption

4. Conclusion

From all our observation and findings, we come to a conclusion that VoIP provides many features but also keeps the way open for the vulnerabilities also. The working mechanism behind the VoIP has been studied and the protocols, basically, SIP has been studied in detail. To avoid any attack, we have to provide some security mechanism which will include the modifications in the underlying protocol architecture. After studying the whole working of SIP and implementing the method, we can conclude that Spoofing can be avoided with the modifications in the SIP itself. The method proposed is the integration of the PKI concepts in order to provide strong authentication which will keep a check from the starting itself i.e from the time of sending the INVITE packet to the callee in order to avoid spoof attacks.

5. References

[1] http://www.voipsa.org
[2]Paul Stalvig "Session Initiated Protocol - A Five Function Protocol"
[3]Rakesh Arora "Voice Over IP Protocols and Standards"
[4] VoIP Think - SIP Example SIP call flow.htm
[5] Rakesh Arora,1999, VoIP protocols[online]. Available: http://www.cis.ohio state.edu/~jain/cis78899/voip_protocols/ index.html
[6] 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
[7]http://searchsecurity.techtarget.com/definition/PKI
[8] http://en.wikipedia.org/wiki/spoofing
[9]http://www.backtrack-linux.org/wiki/ index.php/Pentesting_VOIP
[10] Ge Zhang "Secure SIP Signalling Service for VoIP applications Performance-related Attacks and Preventions".