A Survey on VoIP Security Attacks and their Proposed Solutions

Jyoti Shukla¹, Bhavana Sahni²

¹Assistant Professor, Amity University
²M.tech Student, Amity University

ABSTRACT

VoIP is a communication protocol which is being widely used and voice calls are transmitted over an IP network such as internet instead of Public Switched Telephone Networks (PSTN). VoIP converts voice into digital signal that travels over the internet and the audio output device makes the digital to audio conversation at the receiver side. In today’s time people are using these technologies in their daily life, for communication over the internet but they are not aware with the security issues on VoIP conversation. There are different types of security issues with VoIP conversation. The main focus on this paper is to introduce different security attacks and defense approaches for security attacks on VoIP conversation.

Keywords: VoIP, Security Attacks, Defense Approaches.

1. INTRODUCTION

Voice over internet protocol (VoIP) is routing of voice conversation over the internet or IP based network. The flow of voice data over the internet in the VoIP system firstly human voice must be converted into digitized form. Then it is compressed to save bandwidth and optionally encryption can also be used to protect the conversation from sniffing. Then the voice samples are inserted into data packets to be carried out over the IP networks. Real-time Transport Protocol which defines the standardized packet format for delivering the audio or video over the internet, RTP packet have header field to hold the data and it is needed to correctly re-assemble packet into voice signal on the other end. Then voice packet carried by UDP protocol due to its low overhead. Now at the other end, the process is reversed. Packets are disassembled and put into proper order and data are extracted from the packets and uncompressed it and converted into digital to analog.

Figure 1 Voice data processing in VoIP network [2]

2. VOIP PROTOCOLS & STANDARDS

VoIP has been implemented in various ways using both protocols and standards.

2.1 H.323

H.323 is a recommendation from ITU Telecommunication Standardization Sector (ITU-T) in 1996 that defines the protocol to provide audio-visual transmission over the internet. It is both reliable and unreliable communication, both type of communication provide by the network. H. 323 using the standard for security. H. 235 standard of H. 323 to
provide security, addresses the security issues including authentication, integrity and privacy etc. It also uses the secure socket Layer for transport-layer security.

2.2 Session Initiation Protocol (SIP)
The SIP is an Internet Engineering Task Force (IETF). It is an Application-layer protocol and signaling Protocol which establishes, modifies and terminates the sessions. It is run on Transport Layer Protocol (TCP), User Datagram Protocol (UDP), or Stream Control Transmission Protocol. It is Text-based protocol, including some elements of Hypertext transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP). For security SIP using the two mechanisms: end-to-end and hop-to-hop. In end-to-end protection, HTTP provides the authentication.

2.3 Media Gateway Control Protocol (MGCP)
The Media Gateway control Protocol is “an Internet Engineering Task Force” and it is a signaling and calls control protocol used by VoIP systems.

2.4 Real-time Transport protocol (RTP)
The Real-time Protocol defines a standardize packet format for delivering audio and video over the internet. RTP is specified by IETF. RTP is designed for end-to-end, real time, transfer of data. RTP specified two sub protocols is Data transfer protocol, RTP, which deals with the transfer of real-time data and RTP Control Protocol (RTCP) used to monitor information in an on-going conference. It is used to provide the feedback on quality of services (QoS) being provided by the RTP.

2.5 Session Description Protocol (SIP)
SDP intended for describing multimedia sessions for the purpose of session announcement and other forms of multimedia initiation. When initiating multimedia video conferencing, VoIP calls, or other session. There is a requirement of media details, transport addresses and other session description to the participants. SDP provides the session description of the participants, how that information is transported.

2.6 Jingle XMPP
It is an extension of Extensible Messaging and presence protocol (XMPP) which adds to peer-to-peer session control for VoIP and video conferencing communication. It is designed by Google and the XMPP Standards Foundation. XMPP is a communications protocol for message oriented middleware based on XML (Extensible Markup Language).

3. SECURITY ATTACKS AND DEFENSE APPROACHES
In early days of VoIP, there was no big concern about security issues related to it. People were mostly concerned with its cost and functionality but now days VoIP is becoming a one of mainstream communication technologies, security become a major issue. Attackers target the VoIP application. In this section we present the study of attacks on VoIP conversation and we also discuss approaches that have been adopted to counter the attacks.

3.1 Denial of Services (DoS)
DoS attack is ranked first in the top five VoIP security threats of 2008 (Higdon, 2008). Denial of services (DoS) attack is an attack on a network or device denying it of a service or connectivity. It can be done by consuming its bandwidth or overloading the network. DoS attack is attempt to make a machine or network resource unavailable to its intended users. In VoIP DoS attack carried out by the flooding. This causes calls to drop prematurely and halts the call. Once the target is denied of the service, attacker can get remote control of administrative facilities of the system. There are different types of DoS attack. A VoIP connection is established using two protocols, a signaling protocol and media protocol. Another type of attack is gateway attack, where a gateway acts as a router between different networks.

3.1.1 VoIP Signaling DoS attack [2]
The attacker can attacks on signaling protocol to conducts a Denial of Services attack. In the first type of attack the attacker sends the many “invite” request to bob. At the same time Alice also sends the “invite” request to bob, but bob can’t take request from Alice. In this type of DoS attack does not have same LAN requirement, only needs of large volume of request to flood the victim.
In the second case, the attacker uses cancellation to cancel all pending call set up signals by sending a CANCEL, GOOBYE or PORT UNREQUACHABLE message. The attacker wants to disrupt the phone calls by sending the malicious hang-up messages to the recipient as if they came from the caller. In the fig 2. (b) it shows an example where spoofed CANCEL message by the attacker to prevent call setup. In Fig (c) where GOODBYE message is spoofed by the attacker to prevent call setup or tear down the establish connections. In this type of attack does require the attacker to be able to fill certain header of the correct message. The attacker can gather the network data.

Figure 2(c) Teardown signal DoS [2]

3.1.2 VoIP Media DoS attack

In this type of attack, the attackers can flood the gateway, IP phone and other media VoIP components with large numbers of RTP packets. It is a common and popular way to deny services to users is to flood a network with traffic. When bandwidth is flooded, this can also disrupt VoIP services. Because there is not enough bandwidth or resources left for the normal users of the services. Furthermore the attacker might knock key components like gateway offline.

Proposed Solution for Dos attack [5]

- **Monitoring & Firewalls**
  Filter the unwanted traffic. Maintain the list of unauthenticated and suspicious users and deny those users from establishing sessions. However, filtering induces the time delay that reduces quality of services. VoIP uses an Internet connection and no ‘physical wire’ is needed, it does not have the same security as telephone lines. Interception and disruption don’t need to be physical to cause damage, and these attacks can come from anywhere on the network. That’s why VoIP firewalls are important. They provide the same level of protection for VoIP traffic as ordinary firewalls do for applications and data traffic.

- **Authentication**
  The solution is to configure authentication on VoIP application. To verify the identity of a user before forwarding his/her messages. Authentication may require two communicating VoIP devices to authenticate each other before the actual communication starts. This mutual authentication might be based on a shared secret that is known prior to the communication, making it difficult if not impossible for an attacker to masquerade identities.

- **Stateless proxy**
  To reduce the risk of memory exhaustion attacks (DoS) thus can be used to perform other security checks such as authenticating users, registering third party, and filtering spam sources.

3.2 Eavesdropping

While most of the people are aware of the fact that conversation may be eavesdrop over the Public Switched Telephone network. Users rarely think that someone could listen to their VoIP calls. Through eavesdropping third party can obtain names, passwords and phone number, allow them to gain control over voicemail. Phrase Spotting technique used to eavesdrop on VoIP conversation. In Phrase Spotting Technique rather than eavesdropping on entire conversation the attacker simply wants to find out during the conversation if any specific phrase or word uttered. What makes the attack possible is the Code-Excited Linear Prediction (CELP) [6] technique used by the voice CODEC’s. Most common CODEC’s are based on technique called CELP. In this technique, CELP CODEC’s use the codebooks for mapping the each speech sample to the particular codebook entry which is closest to the original speech pattern then the codebook entry are placed in the encoded VoIP packet and packets are to be sent across the network.
Propose Solution for Eavesdropping Attacks

Long (2002) recommends four strategies to prevent eavesdropping [5]:

- Employing flawless hardware.
- Ensuring that access to wiring closets is restricted to authorize personnel only.
- Implementing port-based MAC address security on any vulnerable network point; for example, on reception courtesy phone.
- Initiating a procedure to regularly scan the network for devices running in promiscuous mode.

3.2.1 CBR CODEC’s

Using CBR CODEC’s is defense approach against Phrase spotting attack. Constant Bit Rate encoding means that the rate at which a codec's output data should be consumed is constant or fixed size packets. If payload is encrypted then the correlation between speech and correspondence bit is completely destroyed and making this attack inapplicable.

3.2.2 VBR CODEC’s

Variable Bit Rate is another defense approach against the attack. This achieved by continuously changing the bit rate during the encoding process on the nature of audio. But this is not completely eliminate the eavesdropping attack.

3.2.3 Padding to a fixed length

This is the technique which completely eliminates the possibility of eavesdropping on a encrypted VoIP conversation. That is padding the each and every packet to a constant length.

3.2.4 Apply Encryption Selectively

Encryption is necessary to defeat eavesdropping attack. Many different algorithm can be used such as DES, 3DES, AES, RC4 and RC5. Transport layer security and IP sec are main encryption methods.

3.3 Packet Spoofing & Masquerading

VoIP can also be realized as a masquerading attack in VoIP networks. Masquerading is type of attack where the attacker pretends to be authorized user of the system to gain access to it or to gain greater privileged than they are authorized for. A masquerading may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through by passing the authentication mechanism. Masquerading attacks can be used to commit fraud, unauthorized access to sensitive information and even service disruption. Perhaps the worst case is that the attackers pretends or takes over someone's identity in the service.

Proposed Solutions for Masquerading Attacks [5]
An effective authentication module combined with encryption would be an effective solution to Masquerading and spoofing attacks. Only authorized user can access the system.

3.4 VoIP Spam and Phishing
Before VoIP became popular, phishing attacks were made through spam email messages. Vishing is another word for VoIP Phishing which involves a party calling you faking a trustworthy organization (e.g. your bank) and requesting confidential and often critical information. Phishing is an attack against data privacy whereby the victim himself gives out his personal data, after biting the bait. Phishing is a type of attack that is gaining popularity now days, and is an easier way for data thieves to obtain what they want. Phishing works like this: a data thief sends you an email message or a voice mail making it seem like it is an official message from a company you have financial or other interests with, like your bank, PayPal, eBay etc. In the message, you are informed about a problem which puts you in alarm and are requested to go to a site or phone a number where you have to give your personal data like credit card number, passwords etc.

Proposed Solution for VoIP Spam and Phishing [5]

- **Filter traffic based on frequency and duration.** A filter can identify calls likely to be spam on the basis of the frequency and duration of the calls. Qovia recently filed two patent applications for this technology designed to thwart spam over Internet telephony (SPIT) (Celeste Biever, 2004).
- **Detection and mitigation of SPIT networks using signaling protocol analysis** uses analysis of the VoIP signaling messages which can assist service providers in detecting spam activity targeting their customers. MacIntosh et al. proposed this solution (MacIntosh et al., 2005).
- **Dantu and Kolan (2004, 2005)** use a voice spam protection algorithm. They utilize user feedback to calculate a caller’s reputation value using a Bayesian inference function, taking into consideration the caller’s past history.
- **Trust enforcement in peer-to-peer (p2p) VoIP networks** uses a trust enforcement framework consisting of computation and memory bound functions that associate trust implicitly to the p2p VoIP entities (Banerjee et al., 2006).
- **Reputation-based spam filtering.** From Rebahi and Sisalem (2005), is a spam-blocking algorithm in which a reputation network manager is built from an SIP repository.
- **Never give any personal information on phone for any reason.** If you need to provide your personal information it is safer to walk to the office or bank for it. Besides all the popular online companies like PayPal, eBay and other institutions like banks etc. Warn users through their websites or other ways that they never ask for any personal information on email or automated phone calls. This should make it a lot easier to tell phishing attacks out.

3.5 Tall fraud
Tall fraud is ability to have unauthorized access to the VoIP services. This is the most critical attack. Tall fraud can be realized by manipulating the signaling messages or configuration of VoIP components. The risks of toll fraud attack within a VoIP network are that some hackers are able to hijack the systems. With VoIP you are sending credentials to someone's device while you call and that device while you call and that device communicates back to you. This communication needs to properly encrypt. Hackers can get directly onto phones and copy the credentials and place them in their own equipment. There are many benefits of VoIP such as cost savings and self-setup. If implemented properly most VoIP systems are truly "plug and play" and do not require a visit from the phone vendor, if the company does not set up the system properly by not following vendor directions then they can exposed to fraud. For example on a machine that does not have simple password and another source of exposure could be the lack of internal best practices such as using "1234" as a voicemail password which is easily guessed and allows backdoor entry to the entire system.

Proposed Solution for Toll fraud
VoIP providers can prevent toll fraud by properly configuring firewalls and by protecting ports. VoIP providers to protect against the fraud threat are to implement sophisticated early detection rules which allow them to suspend service in real-time when a breach is discovered. VoIP providers must also actively monitor who is accessing their network with what frequency and who is generating what kind of traffic.

3.6 SPIT (Spamming over Internet Telephony)
VoIP spam or also known as Spam over Internet Telephony (SPIT) is expected to be a serious problem for VoIP networks. If you are mailing regularly then you must know what spamming is. Spamming is actually sending emails to people against their will. VoIP is not common yet but is starting to be especially with the emergence of VoIP as an industrial tool. Every VoIP account has an associated IP address it is easy to spammers to send their messages to thousands of IP address. Spam messages can carry viruses and spyware along with them. This brings us to another flavor of SPIT which is phishing over VoIP. Phishing attack consists of sending a voicemail to a person and
masquerading it with information from a party trustworthy to the receiver like a bank or online paying service because voicemail usually asks for confidential data like passwords or credit card number.

**Proposed solution for SPIT**

- **Filtering**
  According to Brewton the best course of action for any user who trying to protect his/her VoIP system is to buy filtering technology but while VoIP providers can help filter out obvious SPIT before it traverses a network and there is always a risk of false positive legitimate traffic or large scale message transmissions that accidentally flagged as SPIT and prevented from reaching employees.

- **Firewalls**
  A VoIP firewall is an application driven by a security policy that defines whether to allow or deny certain calls. Administrators set policies through GUIs. A defense approach against threats, firewalls detects and blocks VoIP DoS (denial-of-service) attacks, SIP attacks, toll fraud, virus infections and SPIT.

- **VoIP SEAL**
  VoIP Seal is a new tool that targets calls originating from spam-generating software. SPIT is detected and blocked based on communication patterns observed during the call. If spam related calls comes in the VoIP SEAL will prevent the phone from ringing.

3.7 **Man-in-the-middle attacks**

Man-in-the-middle attack [2] in which the attacker intercepts call signaling SIP message traffic and masquerades as the calling party to the called party and once the attacker has gained the position he can hijack calls.

- Alice sends an invite message to bob and this message are detected by attacker.
- Attacker sends a response message to Alice spoofing from Bob with 301 moved permanently code. In the response Attacker set the new address of Alice to his computer.
- Alice sends a new invite message to Attacker. According to Alice she is connecting to Bob.
- Attacker sends back an acknowledgement to establish the connection between him/she and Alice.
- At the same time, Attacker sends an invite message to Bob and he can fake the caller ID of Alice.
- Attacker replies with 200 ok and the connections between Bob and Attacker are established.

Now attacker can do anything gain. Attacker can also record the content of conversation. This is a man-in-the-middle. Encryption is deployed in both connections; Attacker can still access the whole conversation. Call redirection and call hijacking enables to attacker to eavesdrop even encrypted voice conversation.

![Figure 6: Man-in-the-middle attack [2]](image)

**Proposed solution for man-in-the-middle**

Stronger authentication schemes are the solution to call hijacking. You could have a firewall system randomize TCP sequence numbers, ensuring that it becomes almost impossible for attacker to predict future sequence number for the sessions. The best solution is to use VPN for man-in-the-middle.

- **Device authentication**
- **Packet integrity checking**
- **Encryption**

In device authentication, it assured that the device that is sending traffic to you is an authorized device. It provides the authentication to device instead of a masquerading device. In packet integrity, it can be assured that the packets coming to you are from an authorized source. And in encryption, you can be assured that a man-in-the-middle cannot eavesdrop the voice conversation between two devices.
4. CONCLUSION

The paper outlines security issues and defense approaches for security attack. VoIP have to deal with the security problem. Once the calls are hijacked, It is easier to eardrop the conversation and modify it even Proper encryption is necessary to protect the confidentiality. Attacker can also launch the denial of services attacks by sending large numbers of spoof packets for call setup. They can also send large number of RTP packets. The migration approach is to deploy firewalls and IPS system. VoIP specific Firewalls should be deployed in voice network to prevent the malicious data traffic. VoIP security would be detrimental to public’s confidence in the technology. Defense in Depth is a key of defending VoIP.

REFERENCES


Authors

Jyoti Shukla has done her B.Tech In Computer Science and engineering from V.B.S Purvanchal University, India in year 2002. Later she got MTech degree in IT from GGSIP University; New Delhi, India in the year 2008.She has vast teaching experience of 10 years in various engineering colleges in India such as Amity University, Jaypee and JSS Academy. Currently she is working at Amity University in the department of CSE.

Bhavna Sahni is currently pursuing doing her MTech dissertation at Amity University in Department of CSE.