

Synopsis of Security Threats and Implements in SIP-Based VoIP Systems

Samina Bader-uz-zaman, Fareeha Razzaq, Fozia Arshad, Shahzada Khayyam and Sohail Ahmed

{Adan_dua | Fareeha_razzaq | Fozia_uet }@yahoo.com

{shahzada.khayyam | sohail.ahmed}@uettaxila.edu.pk

University of Engineering & Technology, Taxila, Pakistan

ABSTRACT

Voice over internet protocol is mostly transmitted without encryption so, our communication is insecure because anyone who has access to our LAN can connect his network monitoring equipments and can interfere into our VoIP based telephonic conversations. In this paper possible existing threats in VoIP networks and available tools for its security have been elaborated.

KEY WORDS: DOS, PSTN, VOIP.

I. INTRODUCTION

In the beginning of VOIP its users were mostly interested in its cost, reliability and functionality [1]. So, at that time its security was not a big issue. In the recent years most people prefer to use VOIP and is becoming one of the popular communication technologies. Due to the nature of VOIP calls its protection from various threats has become a big issue.

In short VOIP calls are transmitted over the IP network in unencrypted form, it means anyone who has access to the network between originator and receiver can receive these packets and can create a recording of our private chat.

VOIP data is transmitted in simple digital packets. It means that it can be attacked, manipulated, rerouted, intercepted, hacked and degraded just like packets on the data network [2].

II. VOICE OVER IP

VOIP allows its users to transfer their digitized voice over the internet protocol instead of using traditional circuit switched. VOIP lowers the cost of communication and increases the flexibility for both businesses and individuals. Since the invention of telephone circuit switched networks were used for voice communication. But with the invention of VOIP, IP based packet-switched networks have largely replaced the traditional circuit-switched networks [3].

Following steps will be performed in order to transmit voice over IP.

- Digitize analog voice signal.
- Create packets of the digital signal using TCP-UDP/IP protocols
- Transmit these packets on the internet.
- At the receiver side these digital packets will be reconstructed in the analog form.

III. THE BIGGEST VOIP SECURITY THREATS

1. Dos

In this type of attack, attacker tries to prevent the phone service from operating under normal operating specifications. VOIP service is degraded, when a target is flooded with unnecessary SIP call signaling messages. As soon as the target becomes unable to use the service and stops operating, perpetrator can get control of the system. In a number of ways a Dos attack can affect. Three basic types of attacks are described below:

- i. Consumption of computational resources, for example, CPU time, disk space and bandwidth.
- ii. Disruption of configuration information, for example information related to routing.
- iii. Disruption of components of physical network.

1.1 Flooding of Requests

In the following subsection we will explore the attacks that overwhelm the target with a number of requests that may be valid or invalid.

1.1.1 User Call Flooding

In this type of attack, target is interrupted because a large number of valid requests are forward to the destination that is able to process the requests.

1.1.2 Flooding Destination's Requests

In this type of attack an endpoint can be crashed and rebooted by sending a large number of call establishing messages like SIP INVITE requests. Its result may be to disconnect the already built connection as shown in Fig1.

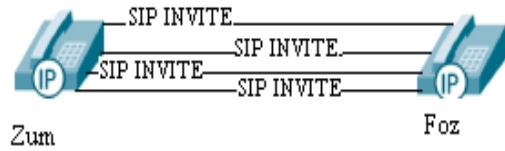


Fig1. Flooding Destination's Requests

1.1.3 Flooding Of Call Controller

In this type of attack Call Controller can be crashed and rebooted by sending a large number of call establishing, messages like SIP INVITE requests. This can disable a large number of endpoints, and they will no longer be able to originate or receive a call as shown in Fig2.

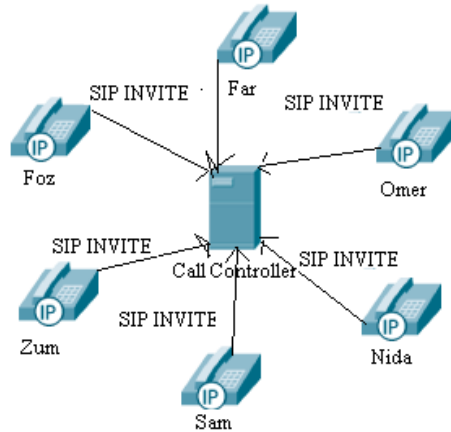


Fig2. Flooding Of Call Controller

1.1.4 Looping of Requests

In this type of attack, attacker affects the two terminals across or within the domain in a way that they start sending the same request message to each other again and again so a loop of requests is formed. Following figure illustrate this concept, where Far and Sam start sending unnecessary INVITE requests to each other. Far Invites to Sam and Sam to Far. In this way a loop will be generated and both systems cease operating as shown in below fig.

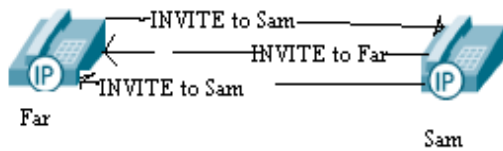


Fig3. Looping Of Requests

1.1.5 Flooding Directory Service

In this type of attack a large number of queries are sent to the DHCP server, directory Server or a DNS server. This could disturb the functionality of the associated server. So the associated end points will be taken out of the service.

2. Fraud /Identity and service theft

Fraud/identity and service theft means that a perpetrator gains access to the network by initiating outbound long distance calls and grasping control of an IP phone.

3. Eavesdropping

Eavesdropping is how most hackers make calls without paying and steal other information. It describes a method by which an attacker can not actually change the data but he can monitor the entire traffic between the two or more endpoints.

3.1 Tracking of Call Pattern

In call pattern tracking, an attacker can analyze the traffic by any means between two or more endpoints on the network.

3.2 Capturing of Traffic

In traffic capturing an attacker records traffic by any means. It includes Packet logging, packet recording and packet snooping for unauthorized purposes. In this type of attack communication is recorded without the permission of all the parties.

3.3 Harvesting Number

It means that a person captures the identity and then it enables other unauthorized communication.

3.4 Reconstruction of Conversation

Reconstruction of conversation means that an unauthorized user monitors, records, reconstructs, stores, recognizes, interprets and translates extraction of features of voice or audio in any type of traffic like presence, status or identity.

3.5 Reconstruction of voicemail

Reconstruction of voicemail means that an unauthorized user monitors, records, Reconstructs, stores, recognizes, interprets, and translates feature extraction of voice mail message like presence, status or identity.

4. Phishing

Criminals can spoof caller identification information so, caller perceives that the call is coming from a genuine organization and then gets identity information from the call recipient.

5. Viruses and malware

VoIP also suffers from worms and viruses. Virus is a set of instruction that, when executed, inserts copies of itself into other programs, while a worm is a program that replicates itself by installing copies of itself on other machines across a network.

6. Call Tampering

It's the type of attack where attacker tempers an ongoing phone call. Perpetrator can insert noise packets in the primitive packets and spoil the quality of the voice.

7. Man-in-the-middle attacks

VoIP is particularly susceptible to man-in-the-middle attacks, in this type of attack perpetrator intercepts call signaling SIP messages and disguise as sender to recipient, or vice versa. Once the perpetrator has gained control, he can hijack calls through a redirection server [4].

8. Directory tampering

- Manipulation of registration can remove, add or hijack the registration of the phone.
- Without the knowledge of caller, calls can be rerouted to another destination.

9. Function and Feature tampering

Without the permission of the administrator features and functions can be enabled and disabled.

- Improper way as the application can be blocked or enabled in the call server.

10. Call Hijacking

Hijacking occurs when an attacker takes over some of the transactions of the VOIP service. After this attack target will no longer be able to access the services from the network.

10.1 Registration Hijacking

In this type of attack an attacker may change the registration messages of the target to redirect the messages to another destination. This makes the target unable to make or receive calls.

IV. SECURITY TOOLS

In this subsection currently available tools for the VOIP security, and their strengths and weaknesses are elaborated.

1. Zfone Encryption

VOIP calls are vulnerable to multiple threats that traditional circuit switched networks are not. That's why encryption for VOIP is so important. Encryption is an essential technology for the security of VOIP. Encryption is the method in which we encode our message using a key so that only the intended person can receive and understand our message and no one else can listen or interpret our calls. Message is decoded at the receiver end using a particular key.

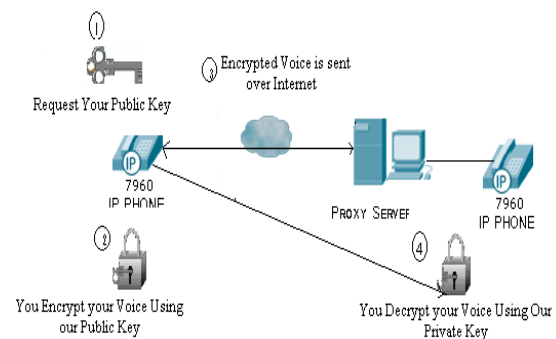


Fig4. Encryption and Decryption of Voice

Zfone is an encryption scheme used for the security of the VOIP calls. It manages the encryption and decryption of the calls and there is no need to store keys in a central server or to get its permission.

Zfone functions with VoIP protocols like SIP, and is simple to use.

We need to install the application at both ends so the encryption and decryption of the VoIP calls could work correctly. If the application is installed only at the caller end and not on the recipient side then call will be treated as regular unencrypted VoIP call. If Zfone is running at both ends then a key will be generated with each new call and each packet will be encrypted and decrypted properly.

Strengths

VOIP calls are transferred over the broad band network and are not secure, so encryption of voice is important so Zfone is a biggest tool in this respect.

Weakness

Currently, it's suitable only for soft phone on Linux and Macs systems.

2. SiVuS

SiVus was the first scanner for the vulnerabilities present in the voip system. It was developed for Microsoft Windows. It consists of three elements:

- Generator of SIP messages: It is used for the testing of the issues.
- Discovery of SIP component: It is used for the identification of Victims for synopsis.
- Verification of the robustness and security:

This component is used for the verification and robustness of the Proxy server, Registrar servers and other SIP based phones.

Advantages

- SiVus scanner is more user's friendly as compared to the other scanners because it was designed using windows based application.
- It tests availability of various security features and the robustness of all SIP message types.

Weaknesses

- It does not contain enough information necessary for the analysis of test output.

V. CONCLUSION

Security is very important for the future of VOIP. One possible solution is to encrypt your voice so that an unauthorized person can not intercept our private conversations. There are

many tools available for the security of VOIP like, Zfone, and SiVuS. After the detailed study of these softwares we come to know that none of these softwares is perfect, each has some strengths and weaknesses. We need to overcome these weaknesses in order to make our private VOIP calls secure.

Most of the same security implements implemented in data networks could not be used in VOIP systems. We need to modify existing tools or develop new tools that can encrypt data as well as voice.

VI. REFERENCES

- [1] <http://fairproxy.com>.
- [4] <http://www.xchangemag.com/articles/06octnewtel0.3.html>.
- [3] <http://ieeexplore.ieee.org>.
- [4] <http://voip.about.com/od/security/a/SecuThreats.htm>.
- [5] D. Richard Kuhn, Thomas J. Walsh et.al. "Special Publication 800-58: Security Considerations for Voice over IP Systems", National Institute of Standards and Technology, Jan 2005.
- [6] W. Rash, "BorderWare Firewall Fights VoIP Threats", the Channel Insider, 14 Sep 2004.
- [7] S. Salsano, L. Veltri, D. Papalilo, "SIP Security Issues: The SIP Authentication Procedure and its Processing Load" Network, IEEE, Vol. 16, Iss. 6, Nov/Dec 2002, p.38- 44.