Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Defence Approach for Eavesdropping Attack on VoIP Conversation

Bhavana Sahni*, Jyoti Shukla
CS&E Department, Amity University
India

Abstract— Voice over Internet protocol has become a popular alternative to public switched telephone network. The flexibility and cost efficiency are the key factors luring enterprises to transition to VoIP. As VoIP technology matures and become increasingly popular so it also gains the attention of the attacker who attacks on the VoIP conversation and wishes to eardrop the conversation. In this paper we first describe the phrase spotting technique used to eavesdrop the conversation and defence approach for eavesdropping attack. In which padding to a fixed length and applying encryption algorithms. To make system more secure from this attack.

Keywords— Security attacks, Eavesdropping attack, Defence approach.

I. INTRODUCTION

Voice over Internet Protocol is a communication protocol and technology that allow user to make phone calls, video conferencing etc using a broadband internet connection instead of analog phone line. Firstly voice signal separated into frames which are stored into data packets and then transported over IP network using communication protocol. VoIP technology has recently become an important part of part of our day to day life; millions of people speak over internet but few of them understand the security issues related to voice communication. While people are not aware of the fact that someone could listen to their VoIP calls. An eavesdropper can detect that specific phrases were used in discussion without ever hearing the actual speech of the user. Phrase spotting Technique used to eavesdrop on VoIP conversation. Phrase spotting technique is harmful to privacy. [1] To make system complete, it would also be rational to implement an encryption scheme based on public key cryptography to transfer the information about the padding length securely
Cryptography Goals:

- Confidential: The protection of data from unauthorized party and transmitted information is accessible only for reading by authorized parties.
- Authentication: the authentication service is concerned with assuring that a communication is authentic and the assurance that the communicating entity is the one that is claims to be.
- Integrity: assurance that the data received are exactly sent by an authorized entity. Only authorize parties are able to modify and stored information.
- Non repudiation: It prevents either sender or receiver from denying a transmitted message.
- Access Control: It is the ability to limit or control the access to host system and application via communication link.
- Availability: Computer system assets are available to authorized parties when need.

Table I Overview of the security concern and impact of the VoIP system

Security Concern	Confidentiality	Integrity	Availability
Denial of Services			✓
Eavesdropping	✓		
Toll Fraud		✓	
Man-in-the middle		✓	
Call redirection	✓	✓	✓
Proxy Impersonation		✓	

II. LITERATURE SURVEY

A. Security Attacks

Security issues are a big concern now days. People are not aware with the different types of security attacks. Attacker can gain access to the system. In this section we present the different types of security attacks

1. Denial of Services: Denial of services (DoS) is an attack on network or device denying it of a services or connectivity. DoS attack is attempt to make machine and network unavailable. In VoIP DoS attack carried out by flooding.
2. Masquerading: Masquerading is a type of attack where the attacker pretends to be authorized user of the system to gain access to it. Masquerading attacks can be used to commit fraud, unauthorized access to sensitive information and even disruption.
3. Toll Fraud: Toll fraud can be realized by manipulating the signalling messages or configuration of VoIP components. Some hackers are able to hijack the systems. Toll fraud is the ability to have unauthorized access to VoIP services for personal or monetary gain.
4. Man-in-the middle: Man-in-the middle (MITM) who is in the VoIP signalling or media path, can easily wiretap, divert and even hijack selected VoIP calls by tempering with the VoIP signalling and/or media path. MITM attack can be used for conducting other sub attacks as eavesdropping and DoS. In which attacker is able to insert, read, and modify messages between two parties without knowing the link between them has been compromised.
5. Call redirection: [3] Call redirection occurs when a call is intercepted and routed through a different path before reaching the destination. The attacker can also spoof the response from the recipient and trick the requestor to talk with the attacker.
6. Proxy impersonation: [3] Proxy impersonation attack tricks the victim into communicating with a rogue proxy set up by the attacker. Once an attacker impersonates a proxy, has a complete control of the call.

B. Eavesdropping

In VoIP, eavesdropping is an attack giving an attacker ability to listen and record the private phone conversation. Users rarely think that someone could listen to their VoIP calls. While people are not aware of the fact that conversation over public switched telephone network (PSTN) may be eavesdropped. Eavesdropping attack is intercepting and reading of messages. Phrase spotting used to eavesdrop the conversation. In figure 1(a) network eavesdropping attack is network layer attack. It is consisting of capturing packets from the network transmitted by other computers and reading the content in which search of sensitive information like passwords. While network device is called a hub is used in local area network technology. It is easier to eavesdrop because its repeats all the traffic received in one port to all other. In figure 1(b) it is a process of examining packets as they are transit between source and destination device. In figure 1(b) shows how eavesdropping works in first step attacker notices the user establishing a connection and authenticates with a username and password. It is also examining the traffic between user and server. Telnet passes the information in clear text, now attacker knows that how log on into telnet server. To execute this attack the attacker must be connected physically to the network somewhere between source and destination.

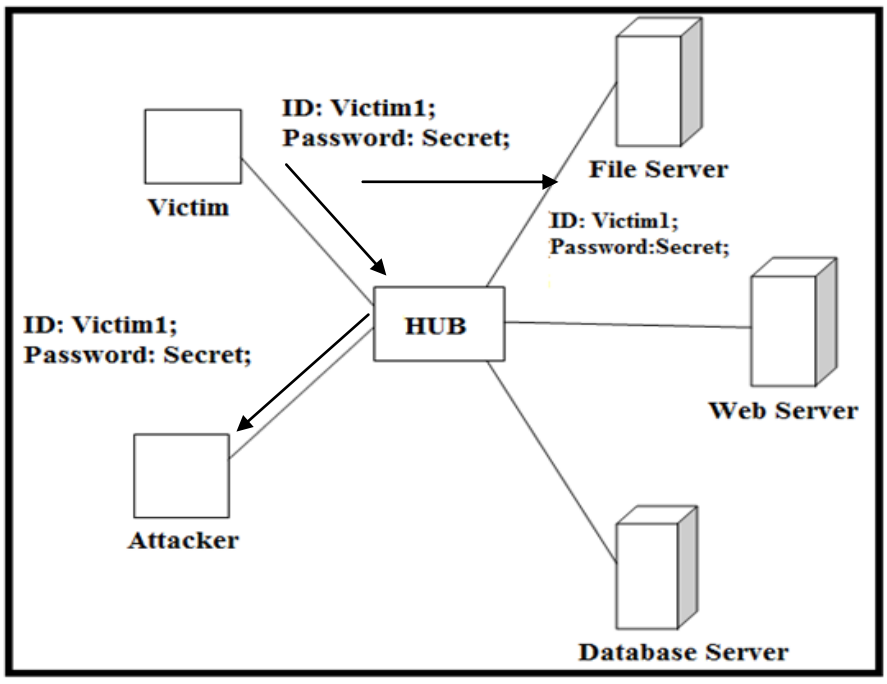


Fig 1 (a) Local Eavesdropping Attack

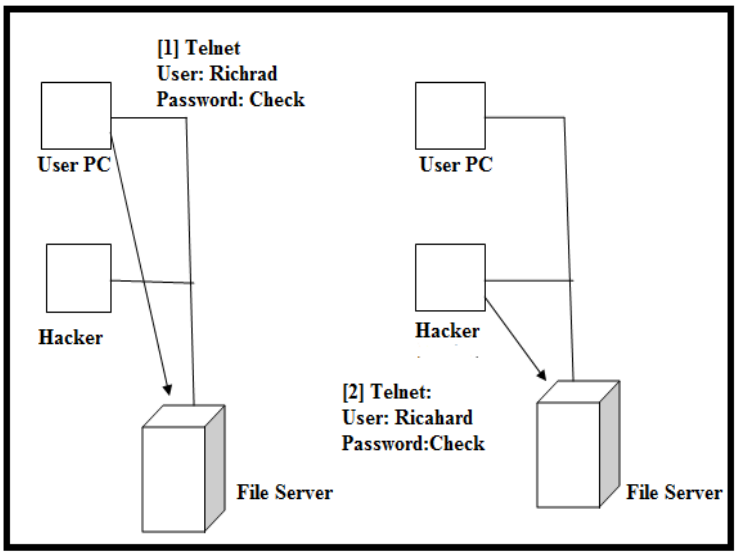


Fig 1(b) Eavesdropping Attack

C. Phrase Spotting Technique:

Phrase spotting technique is used to eavesdrop on VoIP conversation. The logic underlying this phrase spotting technique is rather than eavesdropping on entire conversation, the attacker simply wants to find out if any specific phrase uttered during the conversation. Voice encoding and encryption do not hide all the information contained in the original voice signal. What makes the attack possible is Code-Excited Linear Prediction (CELP). [4] CELP 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.

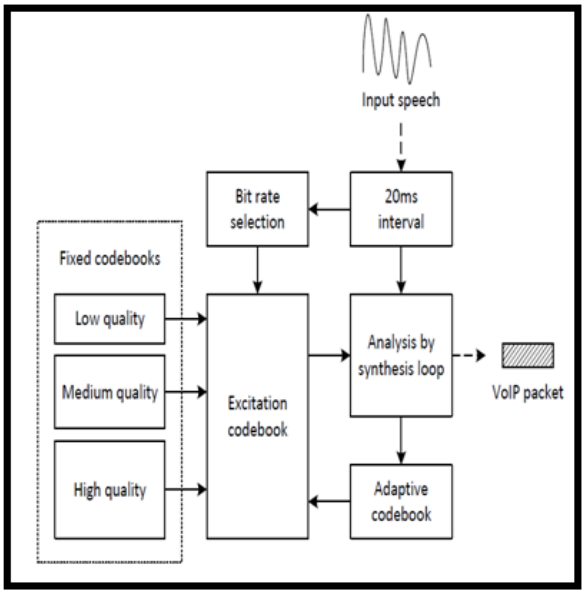


Fig 2 Generic CELP Encoder

III. PROPOSED DEFENCE APPROACH FOR EAVESDROPPING ATTACK

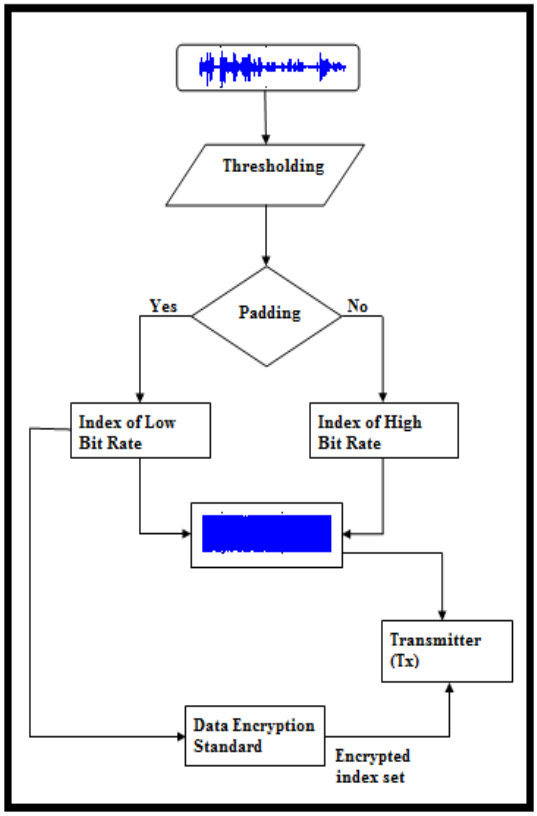
In this section we present the defence approach for eavesdropping attack. It minimizes the chance of attack on VoIP calls. It would also be rational to implement an encryption scheme based on public key cryptography to transfer the information about the padding length securely [1]. A protection technique in which, padding each packet to different value. So that an attacker would not be able to differentiate between low bit rate and high bit rate. Conversation divides into two parts one side is sender and another side is receiver side. At the sender side firstly sender read an audio file, find out the indexes with low bit rate. For securing the conversation, pad the indexes with low bit rate. We are using 10% value of highest bit rate. Add the random noise at threshold indexes with maximum amplitude of highest bit rate. Then apply Data Encryption Standard [5] to all indexes, for encryption and decryption. Then it encrypts the noisy signal and indexes where noise is added. It is symmetric key where both parties share the same key for en- and decryption. At the receiver side, it decodes the noisy signal and removes the noises from the signal. Then get the original audio file. This technique minimizes the attack.

A. *Transmitter*

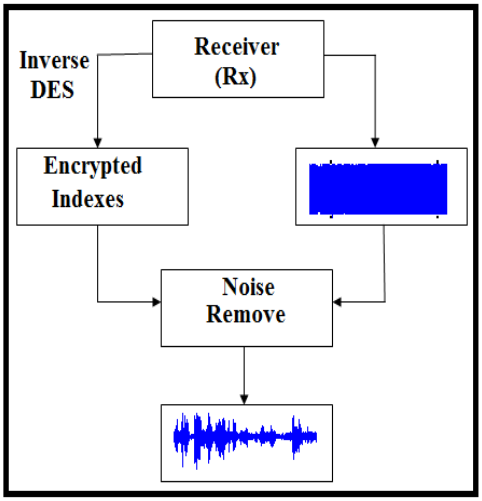
- Read an audio file.
- Then find out the indexes with low bit rate using a threshold schema.
- For simplicity, we are using 10% value of the highest bit rate.
- Then save the indexes of the signal where thresholding is done.
- Insert the random noise at threshold indexes with maximum amplitude of highest bit rate.
- This is the constant bit rate signal which is to be transfer. Let this signal be A
- And then apply Data Encryption Standard (DES) to all the indexes which were thresholded. Let this signal be B
- Then we get two signals that is A and B. These signals will be transfer through the channel.

B. *Receiver*

- Receiver gets two signals. One is DES signal (B) and second is noisy signal (A).
- Decode the DES signal using appropriate key
- The decoded information are the indexes where the random noise is to be remove from the noisy signal
- Remove the noises from the noises signal.
- Then obtain the final audio at the receiver side.



Flow Chart 1 Transmitter Side



Flow chart 2 Receiver side

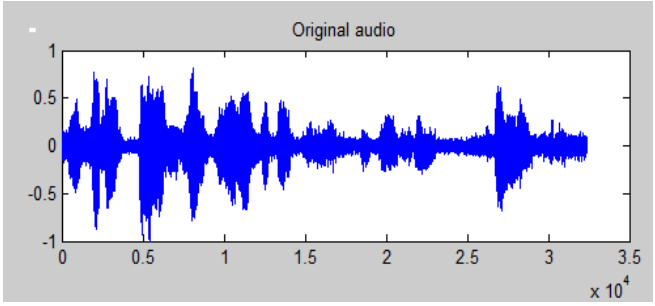
Results: The simulation result is that this technique is applied on 3 different audio files. In the first audio file the no of samples is 32620 and the MSE (Mean Squared Error) value of first audio file is 9.9290e-04 and the threshold is 5 % of highest bit rate.

I

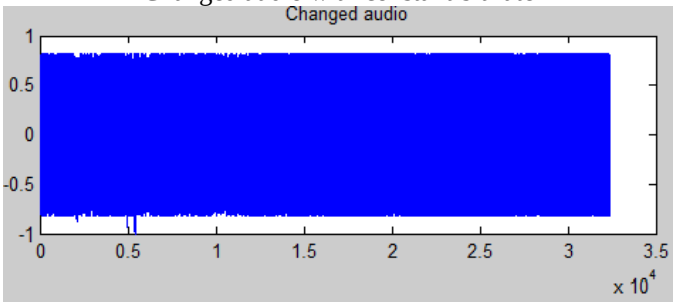
FONT SIZES FOR PAPERS

No of Samples	Threshold			
	5	10	15	20
32620	9.9290e-04	9.9290e-04	0.0056	0.0056
65535	0.0056	2.8449e-04	2.8449 e-04	2.8449 e-04
65535	5.1521e-04	5.1521e-04	0.0057	0.0107

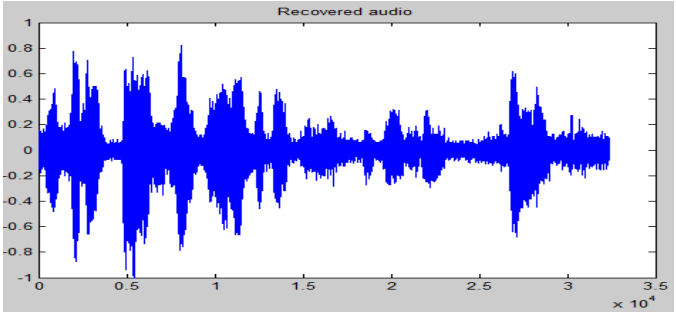
Original audio



Changed audio with constant bit rate



Reconstructed audio



IV. CONCLUSIONS

In this paper we present the technique against eavesdropping attack. We have come to the conclusion that the most promising approach is to find out the low bit rate indexes and then pad the packets with constant bit rate and by using DES (Data Encryption Standard), encryption and decryption the packet. And remove the noise then reconstruct the audio file. The simulation is in MATLAB which gives the MSE value. We generate a table of 3 samples and obtain the Mean Squared error value at 4 different thresholds for each sample. At the lowest threshold, the value of Mean Squared error is low. MSE value is different at different threshold but obtain the less error at lowest threshold. This approach minimizes the possibility of attack. And to make system more secure. It secures the conversation. In the future work it would be logical to enhance our simulation, by using any other algorithm which is better than DES.

REFERENCES

[1] Vaisly Prokopov, and Oleksii Chykov, "Eavesdropping on encrypted VoIP conversation: phrase spotting attack and defense approaches," 2011.
[2] David Bbutcher, Xiangyang Li, and jinhua Guo, "Security challenges and defense in VoIP infrastructure", IEEE transactions on systems, man, and cybernatics, vol. 37, NO. 6, November 2007.
[3] Jianqiang Xin, "Security Issues and Countermeasure for VoIP," SANS Institute, 2007. (Technical report style).
[4] Jyoti shukla, bhavana sahni, "A Survey on VoIP Security Attacks and their Proposed Solutions", IJAIEM, volume 2, issue 3, March 2013.
[5] Jawahar Thakur, and Nagesh Kumar, "DES, AES and blowfish: symmetric key cryptography algorithms Simualtion based on performance analysis", volume1, Issue 2, December 2011.

