International Journal of Advanced Research in
Computer Science Engineering and Information Technology
Volume: 3 Issue: 2 25-Aug-2014,ISSN_NO: 2321-3337

A EAVESDROPPING HARASS OVER ON WIRELESS TECHNOLOGY USING VOIP

A.ANITHA,
Assitant Professor, Dept.of.Computer Appplications,
Bon Secours College For Women, Thanjavur, India.

ABSTRACT–*This paper explains the eavesdropping harass over Wireless networks using VoIP, one of the confidentiality harass. It will clarify the difference between wired and wireless networks and it will explain the related issues to the wireless one using Voip. 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 The illustration will start taking place from defining the eavesdropping, passing by posting the hardware devices and the software tools responsible of achieving that mission continuing thru mentioning the reasons that makes a Wireless network vulnerable and consequently the steps to follow in order to secure it and what is the work done by the Wireless equipment makers to enhance the protecting of their wireless; The paper will continue to specify the difference between legally and illegally eavesdropping.*

Keywords: VoIP, Wireless network, eavesdrop PSTN.

I.INTRODUCTION

Eavesdropping is the process of gathering information from a network by snooping on transmitted data. And to eavesdrop is to secretly overhear a private conversation over a confidential communication in a not legally authorized way. The information remains intact, but its privacy is compromised. It can take place over wired networks as over wireless networks. On wired network the operation of eavesdropping is more difficult because it needs the eavesdropper to tap the network, using a network tap which is a hardware device that provides a way to access the data flowing across the network. And

that of course can't be achieved unless the eavesdropper can be in touch with the wire of the network which is difficult sometimes and impossible the other times. Eavesdropping can also take place on wireless networks where the eavesdropper is not obliged to be in the dangerous position of being compromised. All what he needs is a computer supplied by a wireless network adapter working on promiscuous mode to allow a network device to intercept and read each network packet that arrives even with other network address, to be in the area of the wireless network coverage and to have one of the particular software tools that allows the eavesdropping over wireless network. An example of eavesdropping is intercepting credit card numbers, using devices that interrupt wireless broadcast communications or tapping wire communications which is the preferable for eavesdroppers.

Eavesdropping can be useful by capturing none encrypted data or known decrypted, encrypted data, but it will be none useful if the data was encrypted by unknown encryption. 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. An eavesdropper can detect that specific phrases were used in discussion without ever hearing the actual speech of the user.

II. AUTHORITY OF EAVESDROPPING DEVICES

An Eavesdropping device is electronic equipment allowing the interception of audio communications, visual images and data. For example: e-mail messages sent and received, names and content of Web sites visited and any downloaded files.

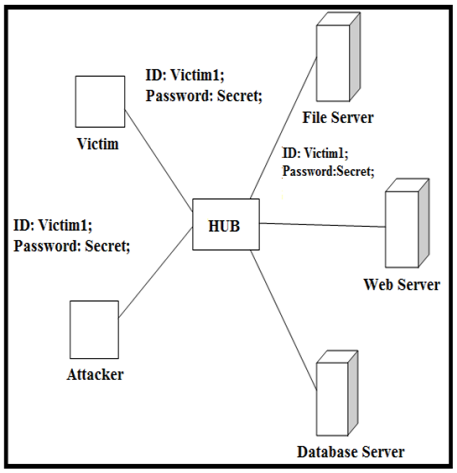
Most eavesdropping devices are sold over the Internet but before you buy any, you should know that it is a crime in most countries to eavesdrop on someone's privacy and you should be aware of the legal issues because some are not legal to own, while others are legal, like those that may be used to record your own conversations with someone.

III.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 it a process of examining packets as they are transit between source and destination device. It 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.

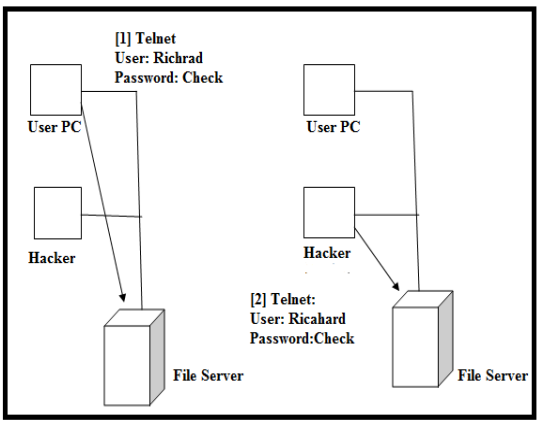
IV.APPROACH FOR EAVESDROPPING ATTACK

In this section we present the 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. 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.



Local Eavesdropping Attack

Then apply Data Encryption Standard 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.



Eavesdropping Attack

V. SIMPLE STEPS TO SECURE WIRELESSNETWORK

Following a few steps can provide some security to Wirelessnetworks:

1. Change the Administrative Password on your Wireless Routers

Routers came with default password from producers to provide easy access, and changing those passwords, is one of the first recommended steps to do, because those default passwords are posted on the vendor support sites, they should therefore be changed right away.

2 .Installing a Firewall

A firewall which is the fence of your network from any unauthorized accessing can help protect your PC by blocking or allowing the pass to your network.

3. Change the Default SSID Name and Turn off SSID Broadcasting

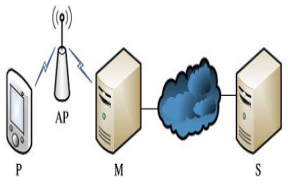
In Wireless LAN computer networking, a service set identifier (SSID) is a code attached to all packets on a wireless network to identify each packet as part of that network. This will necessitate your wireless client computers to enter the name of your SSID by hand before they can connect to your network. But even though and because the data packets that are transmitted will include the SSID it will be easily discovered.

4. Disable DHCP

Disabling DHCP (Dynamic Host Configuration Protocol), and assigning IP addresses to your client computers manually will allow restriction access to the router to specific MAC addresses.

5 .Replace WEP with WPA

WEP (Wired Equivalent Privacy) is a security protocol, encrypting data transmitted over the wireless computer network to provide security and privacy, and to protect the vulnerable wireless link between clients and access points. But as WEP is weak and can be cracked in about 3 minutes as the FBI showed in 2005 using some freely access tools, WPA (Wireless Protected Access) which is more powerful using 128-bit encryption keys and dynamic session keys, must replace it to provide strong data protection.



Wireless man-in-the-middle setup. (P) Phone. (AP) Access point. (M) Man-in-the-middle. (S) Service provider.

VI.WIRELESS EAVESDROPPING EXPERIMENT

In this part I'll present a real experiment to proof the effectiveness of eavesdropping over a non secure Wirelessnetwork.

6.1 Experiment setup

Two laptops, one desktop and wireless router were involved in this experiment. We will name them "A", "B", "C", "D". "A" is Toshiba Laptop, Centrino 1.7 GHz, 1 GB Ram, 80 GB HD and Windows XP Professional as an Operating System. It's the Victim host. "B" is HP Laptop, Centrino 1.7 GHz, 512 MB Ram, 60 GB HD and Windows XP Professional as an Operating System. CommView for Wireless(packet sniffer and generator) was downloaded on this host. It's the Intruder host. "C" is an

IBM server desktop, Xeon 3.00 GHz, 1 GB, 80 GB HD and Windows 2000 Advanced Server as an Operating System installed on VMware ver 4.0. This server has the following application: MS-IIS web server, SMTP Relay service, FTP service. It's the server that the victim will communicate with. "D" is a Netgear 54 wireless router XG614v7, 4 ports UTP switch (Intranet server is connected via), the SSID name is Stay Away, the channel used is channel 2 and the router acts between the wireless network and the intranet server without any security option. It's the AP thru where all the communication of our experiment will take place.

6.2 Hosts Installations and Configuration.

To setup our system environment we needed to install and configure several programs on the different machines. It includes the following:

62.1. Installing and configuring Access Point (Netgear) including:

6.2.2. Installing and configuring Intranet Server including:

6.2.2.1 Installing IIS, SMTP and FTP

6.2.2.2 Configuring IIS, SMTP, FTP

6.2.3. Installing and configuring Intruder Machine.

6.2.3.1 Installing CommView for Wi-Fi

6.2.4 Installing & Configuring Victim Machine

6.2.4.1 Configuring Outlook Express email client

6.3 Experiment Scenario

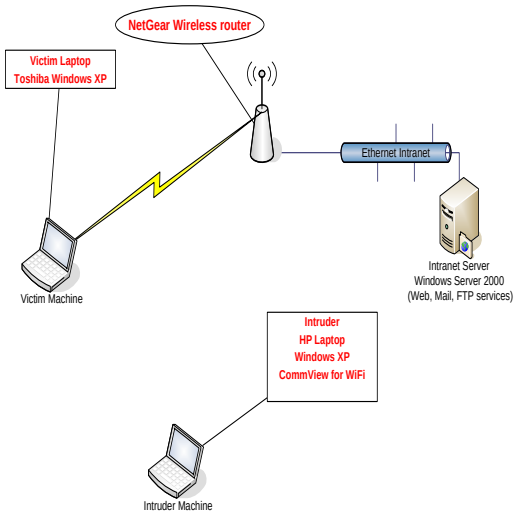


Fig. The experiment Scenario

Before the eavesdropping harass will take place on the victim host "A", the CommView sniffer on Host "B" should be run in order to configure the channel, the IP aliases and the CommView rules (such as IP addresses, Protocols and Ports). After the configuration was done, the harass starts by starting the scanning operation to capture the AP's available in order to start sniffing the packets of a chosen AP.

CommView, at this point, is able to capture all the packets of the configured Protocols, like (HTTP, FTP and SMTP).

Host "A" will start it's communication with the intranet server by demanding an HTTP service to access a webpage. As Host "A" accessing the webpage, the intruder receives all the packets of that service, and consequently, CommView transfer and display this webpage.

Now the victim is trying to download a file from the intranet server by using the FTP service. Typing the user name and the password and after the verification, downloading the file. The entire above service packets have been captured by the

Intruder. CommView again is doing its job. Here is the username, the password and even the content of the text file downloaded.

Host “A” at the end, sent an email thru the intranet server using the SMTP service. But the intruder captured the details of that e-mail.

6.4 Experiment results

Four kinds of different data have been captured by the eavesdropper; Displayed Websites, User name and Password used to access the intranet server, the contents of downloaded files and all the e-mails that have been sent.

All the packets which were sent by the victim as well as the intranet server were captured by the intruder without any loss. By changing the security option of the router from none to WEP, zero packets were captured. .

VII. CONCLUSIONS

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 encryption and decryption the packet. And remove the noise then reconstruct the file. Legality of hardware devices as well as eavesdropping was one of the subjects that this paper talks about. It mentions the hardware devices and the special characteristics that it should have as well as the software tools to be used in order to achieve the harass. At the end we detailed a real experiment which was done, and where the harass proved its capabilities in capturing different kind of packets like HTTP, FTP and SMTP.

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. The same experiment was conducted again but this time the level of security was WPA. The intruder became more upset as he wasn’t capable to capture even a single packet. At the end we have to wish that the WPA security can withstand for a long time.

VIII. REFERENCES

[1] M. Domenico, A. Calandriello, G. Calandriello and A. Lioy. Dependability in Wireless Networks: Can We Rely on WiFi?. IEEE Security and Privacy, 5(1):23-29, 2007

[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].Eavesdropping on Wi-Fi, chapter 6 page 122

[6] The experiment Scenario figure, Eavesdropping project.