

# **Vulnerabilities of VoIP Communications**

**(A white paper on VoIP vulnerabilities and the need of physical layer Security)**

**Dr. Suresh Nair  
P K Radhakrishnan  
Samuel Varghese  
Sreekumar V.M.**



**Plot No.2, Cochin Special Economic Zone  
Kochi-682037.**

**Abstract:**

The document tries to discuss the security vulnerabilities of VoIP Based communication systems, the typical software used for an attack and how physical layer security is most important especially on fibre networks. The paper also includes a demonstration of the VoIP eaves dropping using commonly available software tools and about fibre sentinel system that addresses the physical layer vulnerabilities in optical network.

**Introduction**

VoIP is increasingly used in our enterprises which offer several advantages from the conventional system. As we know, VoIP offers tremendous cost savings since single network is utilized. VoIP Calls also provide location independent services and better utilization of the available bandwidth. The wide spread use of VoIP has also enlisted more security risks on the VoIP calls. The paper discusses the common tools that hackers use to eaves drop the common VoIP Protocols and hack in to the system

**Protocols in VoIP Calls**

There are different protocols that facilitate a VoIP call, the first one being the call signalling protocols. The most common call signalling protocols used for VoIP are SIP (Session Initiation Protocol) defined by the Internet Engineering Task force (IETF) and the H 323 protocol defined by the international telecommunication Union (ITU). These protocols basically identify the VoIP device on the other end to effect communication between them. Either of these protocols is used in any VoIP networks.

**SIP Protocol**

SIP is one of the most commonly used VoIP Voice signalling protocols worldwide. The ease of deployment and seamless integration with existing network has enabled it to be increasingly popular.

The next set of protocols that facilitates a VoIP is the Gateway protocols that connect the VoIP networks to the PSTN Networks. Commonly used protocols for this layer are Media gateway Control Protocol (MGCP) and H 248 called the media gateway controller.

Another set of protocols that comes into VoIP networks are the RTP or the Real time Transport protocols. RTP is a standard for transmitting audio as well as video over IP networks.

Apart from these, several proprietary protocols defined by several service providers are used to enable VoIP networks. The common examples are Skinny Client Control Protocol (SCCP) from Cisco and several others, from providers like Skype.

## Security vulnerabilities in each layer

The common VoIP Protocols like SIP are increasingly exposed to security vulnerabilities since they don't incorporate security technologies like Encryption and Authentication properly.

### SIP Server attacks

The common attacks that SIP Servers are exposed to are

- 1. Message Flow attack :** The SIP specification mentions ways to terminate the session, cancel and invitation and to redirect calls. The improper authentication mechanisms employed in the SIP can be utilized by an attacker to re direct a call or to launch a denial of Service attack. (DoS).
- 2. The Bye or Cancel attack:** The type of attacks uses the "BYE" request to tear down a session. The Bye/Cancel attacks are possible only because the session parameters like the session ID are, by default, exposed to any one and hence any intruder can sniff the network to get the session ID and terminate the session.
- 3. The Re-Invite attack:** These types of attacks utilize the Re-invite Parameter of the SIP. The Re-invite is actually used to update the address/ports of the ongoing call. An attacker can easily send an anonymous Re-invite attack to cause Denial of service or redirect call.
- 4. The INFO Attack:** When the SIP is utilized as a bridge between PSTN Networks, The INFO method is used to send the DTMF Signals, PSTN Signalling messages and even account balance information. An attacker can gain access using the INFO method that enables him to access unauthorised calls, DoS and even billing errors.

The above list clearly depicts the security vulnerabilities in a standard SIP Protocol. Although some of these vulnerabilities can be addressed by using IPSec and other secure tunnelling protocols, some of them are still exposed to risk and yet to be addressed by the current security technologies.

### RTP Attacks

Now let us discuss some of the security risks of the RTP protocol that is actually used to carry the audio and video data over the IP based networks.

- 1. Denial of service Attacks :** The attacker gets the knowledge of the IP and the ports by examining the SIP packets. He uses this information to flood the server /client PC with loads of RTP data. As we know, RTP requires high bandwidth to very huge bandwidth when transmitting uncompressed video data. This exposes the client System to a data flood and hence seizing him from operating any network related applications and thus causing Denial of service.
- 2. Eavesdropping:** The usage of software tools like Ethereal /Wire shark can sniff the RTP as well as SIP Packets to decode the content and filter out the VoIP calls.
- 3. ARP Poisoning:** This type of attack is used to divert the network traffic so that the attacker acts like a man in the middle. He can eaves drop or kill the packet as he requires.

- 4. Manipulation of Gateways:** As discussed earlier, gateways are used to connect PSTN networks to IP Networks. The manipulation of gateways and the protocol (MGCP) will enable the attacker to analyse RTP traffic, forward the RTP packets to another user and uses tools like Robust Audio Tool (RAT) to inject RTP Streams to the network.

### The need of Physical security

We have discussed various vulnerabilities that are already present in the commonly used protocols that enable VoIP Communication. Although secure protocols are being introduced like SRTP (Secure Real time transport protocol), the payload for the authentication hashes are much higher and real time traffic of the data may be impossible when implementing highly secure software tools. Added to these, some of the above mentioned vulnerabilities are not even addressed by the SRTP and other newly developed secure VoIP protocols.

So summarising the above, we may state that

1. The vulnerabilities addressed by the newly developed secure protocols are limited and newer vulnerabilities are coming up which needs to be addressed.
2. The payload on bandwidth for enabling secure VoIP networks is much high.
3. Some special network architectures are required to address every vulnerabilities like implementing IPsec, Firewalls and effecting use of secure tunnels. This automatically increases the costs of the solution. Moreover, newer threats develop which needs to be addressed in real time which may become impossible.

The need of physical layer security comes into picture in this stage where effective isolation may be provided at the physical layer to exclude the hackers. It has been already shown that even fibre optic links are insecure and prone to eavesdropping and attack into the network.

### Demonstration of the Security Vulnerability over VOIP Network

This demonstration shows the vulnerability of the VOIP Network using SIP as the call Signalling protocol and RTP as the media transfer protocol.

The network architecture employed is shown in Figure 1, which consists of two systems which communicate each other, A SIP Server that enables the VOIP Communication and an intruder System that has software installed to sniff the VoIP Traffic.

### SIP Server

The VoIP communication between System A and system B is established using the SIP Server. Several Open source SIP Servers are available in the market and one such SIP Server is SER (SIP Express Router), which runs on both Linux and Windows. For our Lab experiment, we used OnDo SIP server. The onDO SIP Server is configured to enable VoIP Communication between System A and System B.

System A is connected to System B through a series of Optical Fibres and Media convertors in between. This is done to show the vulnerabilities of the Optical network as physical layer.

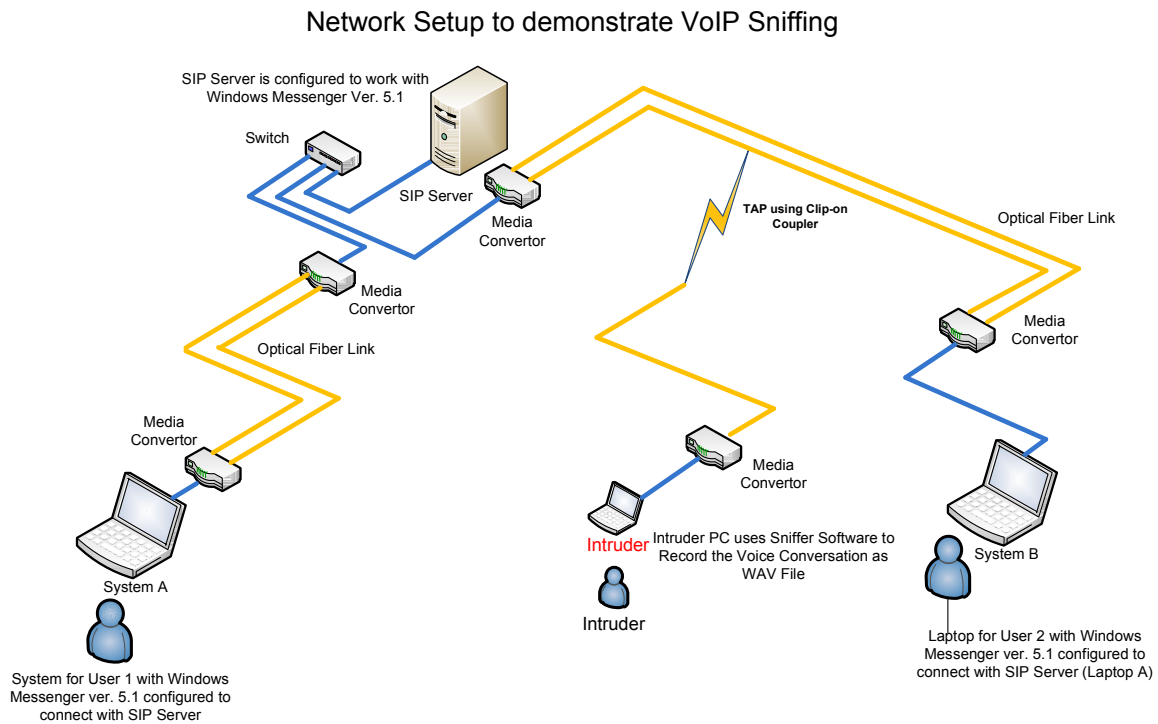


Figure 1

### VoIP Client

The VoIP Client used is the popular Microsoft MSN Messenger 5.1 which can be configured to use SIP Server. The MSN Messenger 5.1 is installed in both System A and System B and a Voice communication is established between them through the SIP Server.

### Intrusion

The intruder system is a normal windows based machine which has sniffer software installed. A series of sniffing software like Ethereal & Cain & Abel are configured on the system to enable VoIP Tap. These softwares are easily available over Internet and most of them are open source/Free. A hacker can easily get access to this software. The installation is also quite simple which may be done even by a novice.

### VoIP Tap

The intruder needs access to the optical fibre link through any means. This may be done through an inexpensive device called Clip – on coupler. The Clip-on coupler will leak out some optical signal from the main stream and media convertors can easily decode the data from the optical signal coming out of the clip – on coupler. The clip on coupler is a form of tap and the victims will have no information about the optical tap being done on the network.

The Optical signal coming out of the clip on coupler is given to a media convertor and the data is converted back to Ethernet format. The sniffer software will make the intruder PC as a promiscuous node which accepts all the data. The Software like Cain & Abel can do ARP Poisoning and redirect the packets to the system. It can also act like a “Man in the Middle”. Here the software filter out the Voice data (RTP data) and converts it to media files like WAV file. Figure 2 shows a screen shot of the sniffer software, creating Wav files out of live VoIP calls.

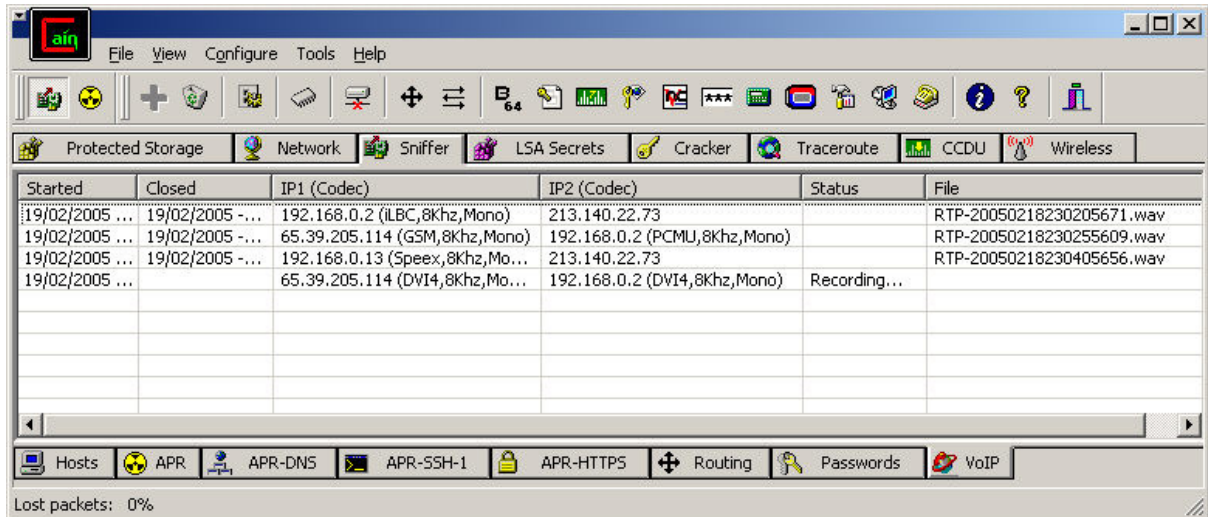


Figure 2

The demonstration clearly depicts the vulnerability in VoIP Communication especially using SIP and RTP as the protocols. This clearly depicts the importance of a physical security layer in any network systems.

### Fibre Sentinel System

Opterna’ s Fibre Sentinel system (FSS) , addresses the vulnerabilities at the physical layer of optical networks. It successfully captures any interruptions caused on the physical layer and inform the administrator about the status of the same. Moreover, it automatically switches to the backup path (if configured to do so) thus protecting the data from the hands of hackers. Moreover, the FSS uses artificial intelligence to categorize the caused interruption into eight categories like transients, Power injection, Tapping etc. An administrator can easily monitor the same in a console even remotely. Please refer to the technical brochure of FSS for more detailed information.

### Deployment of FSS

Figure 3 shows the typical deployment schema of Fibre sentinel system. The FSS works in pairs to monitor the fibre optic system. It sends unique digital signatures between FSS pairs to effectively monitor the fibre optic pair for its health and switches to the backup path when the primary link is under treat. The administrator is warned about the event. Only an administrator can revert the connection back to the primary link. This happens in real time and the switching is done within milliseconds so that the user is unaware of any change in the network. Transients and optical injections are also detected by the system and administrator can set the sensitivity of the system.

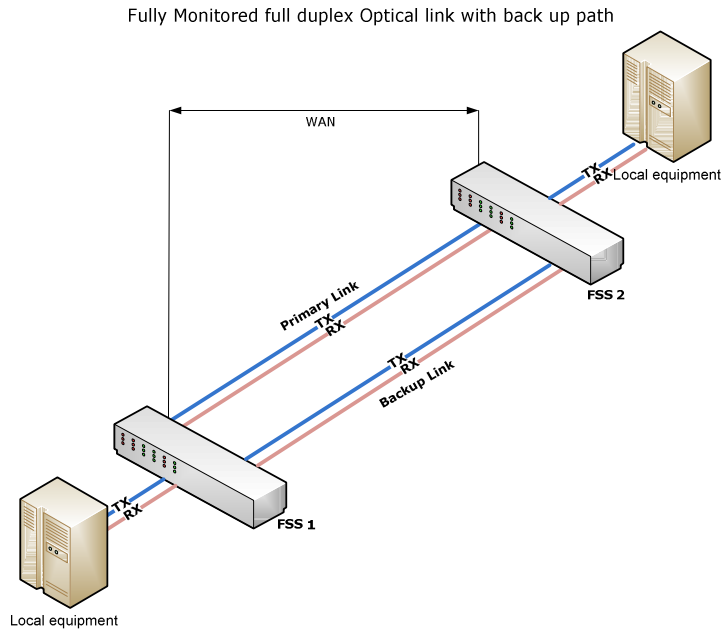


Figure 3

## Summary

The white paper tries to discuss the vulnerabilities of VoIP networks, the ways the hackers use to hack into a system and a demonstration on tapping a SIP based VoIP voice call over an optical network. The importance of physical layer security is established and discussed. FSS, a product from SFO technologies, that provides physical layer security is also discussed.

## Bibliography:

1. Securing VoIP Networks: Threats, Vulnerabilities and counter measures by *Peter Thermos and Ari Takanen*
2. A paper on fibre optic physical layer security by Dr. Suresh Nair, Director NeST R & D
3. Technical user manual Wire shark, Ethereal, Cain & Abel and WinpCap