

# **A Primer of Voice Over IP Insecurities**

## **Introduction**

Voice over IP, or VoIP, has been a technology that has been steadily gaining market share within private corporations, telecom companies, and with end users on the Internet. What many people don't realize is that the de facto standard protocols used in VoIP make it practically trivial for people to eavesdrop on telephone conversations. The purpose of this document is to provide some basic insight into how VoIP works, and show how somebody could listen to your phone conversations. This paper will show a proof of concept for listening into a phone conversation.

## **What is Voice Over IP (VoIP)?**

VoIP is a method of voice communications that encapsulates voice signals in TCP/IP packets. The concept of VoIP began in 1973 with the creation of the Network Voice Protocol on ARPANET. Network Voice Protocol, or NVP, was a process of transporting voice signals over a packetized network. Fast-forward 22 years to 1995; ARPANET is not longer just a research and development network funded by the Department of Defense. It is now the Internet. The Internet is a publicly available network. Just about anybody in the world can get on the Internet and NVP has been transformed to a semblance to what we know as VoIP today. In 1995, a company called "Vocaltec" released a software package called "Internet Phone" and enthusiasts realized how valuable sending voice communications of the Internet could be rather than over the regular phone network.

## **What is SIP?**

SIP stands for Session Initiation Protocol and it is the protocol responsible for registering and finding users, along with setting up VoIP calls. Basically when your VoIP phone connects to a VoIP phone system; SIP is responsible for registering your phone on the phone system, directing calls to your phone for incoming calls, directing outbound calls to the requested phone number, and negotiating the terms of a session.

## **What is RTP?**

RTP stands for Real-time Transport Protocol and is the actual protocol that provides the end-to-end delivery of the voice packets between phones. Once a call has been initiated, SIP hands the data to RTP, which is the actual protocol that is used to move voice packets back and forth between VoIP phones.

## **A basic run down of how VoIP works**

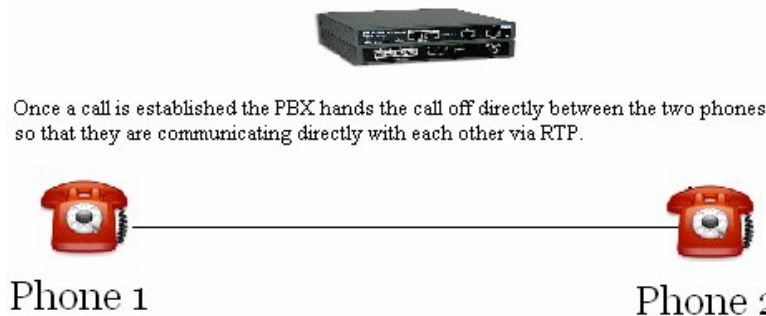
When a VoIP phone connects to a VoIP phone switch the phone uses the SIP protocol to register itself with the switch. Once a user tries to initiate a call with the phone; the phone uses the SIP protocol to communicate with the phone switch to try to locate the destination device.

## VoIP PBX



When the destination device is found by the switch, the switch will try to establish a conversation with the destination phone. Once the destination phone picks up the switch leaves the conversation and the phones communicate directly with each other via RTP.

## VoIP PBX



### **How can VoIP calls be intercepted and re-played?**

VoIP calls are nothing, but UDP packets being sent over a network to a destination. Pretty much just about how everything else works on an IP based network, right? So the question should be: How come I can't use a packet sniffer to gather VoIP data, and is that data sent over the wire in the clear, or without encryption? The answer is you can gather VoIP data and today's packet sniffers even have built in applications that will let you replay the conversation at hand. Refer to Appendix A for an screenshots and a link to the extracted audio for how the VoIP conversation was intercepted and re-played.

### **Conclusion**

While VoIP is a very handy technology that can be used to reduce the cost with many aspects of telecommunications, it does have some down falls when it comes to the privacy of the phone conversations.

### **References**

<http://www.ethereal.com/> / <http://www.wireshark.org/> - Ethereal and Wireshark are technically the same application, but recently the developers of Ethereal decided to change the name of the application. Wireshark and Ethereal are packet sniffing applications that are used to analyze and troubleshoot network communications.

<http://www.faqs.org/rfcs/rfc3261.html> - RFC 3261 - SIP: Session Initiation Protocol - This is the RFC to SIP. This document provides information on how SIP works in excruciating detail.

<http://www.faqs.org/rfcs/rfc3550.html> - RFC 3550 - RTP: A Transport Protocol for Real-Time Applications - This is the RFC to RTP. This document provides information on how RTP works in excruciating detail.

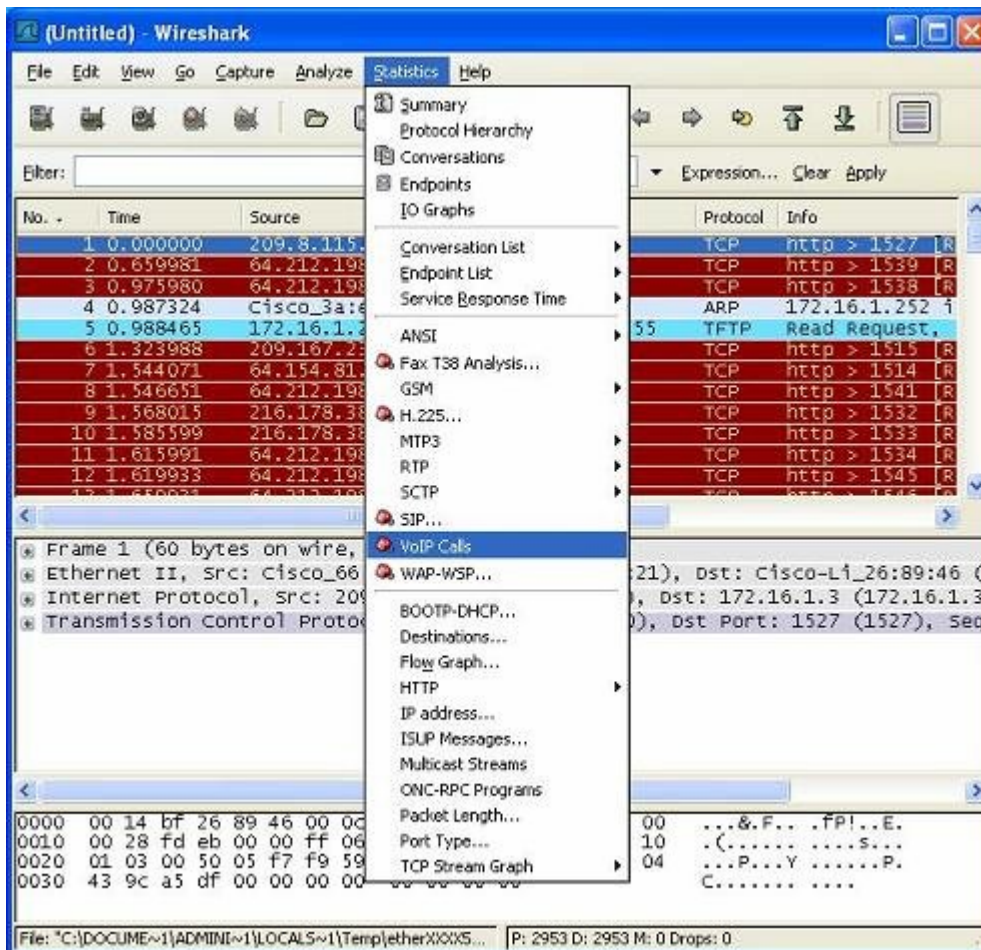
[http://en.wikipedia.org/wiki/Network\\_Voice\\_Protocol](http://en.wikipedia.org/wiki/Network_Voice_Protocol) - A little more insight to Network Voice Protocol.

Book: "Practical VoIP Using Vocal": ISBN: 0-596-00078-2 – Chapter 7: "Session Initiated Protocol and Related Protocols"

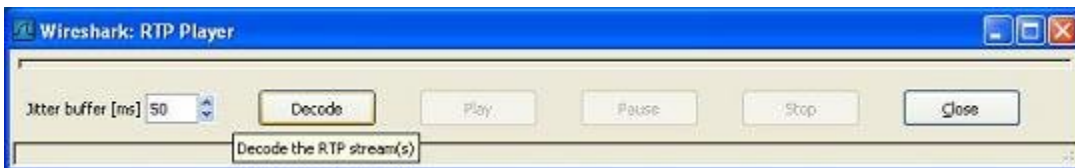
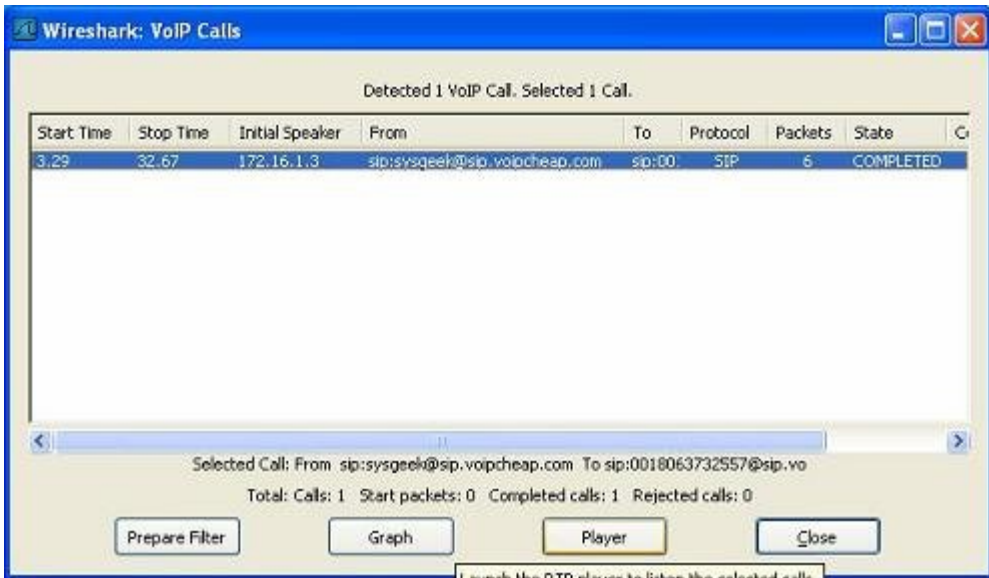
## Appendix A

Here is an example of how Wireshark can be used to sniff and play VoIP conversations:

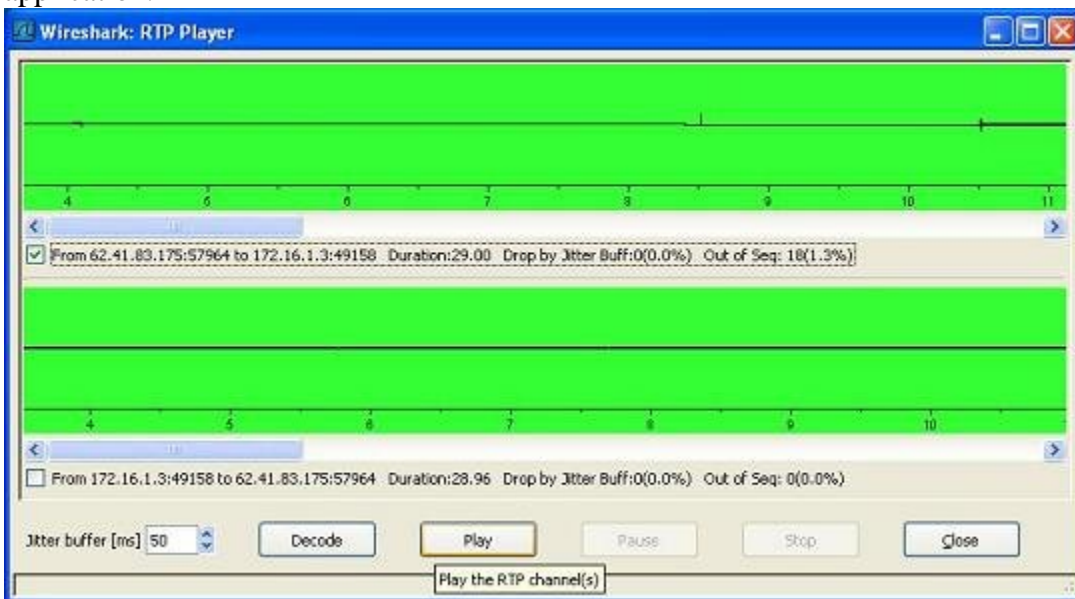
This first screen shot is after traffic has been captured and we are using Wireshark to filter out the VoIP conversation.



Once the VoIP conversation has been filtered from the rest of the traffic you can use Wireshark to decode the data into a voice stream. The next two screen shots demonstrate this.



This last screen shot allows us to play a voice stream live within the Wireshark application.



Here is the link to the sniffed voice conversation, which has been exported to an audio file:

[http://www.securitygeek.net/papers/voip\\_insecurities\\_docs/voicepayload.au](http://www.securitygeek.net/papers/voip_insecurities_docs/voicepayload.au)