Sipera Systems

Advancing Video Attacks

with video interception, recording, and replay

Defcon 17
July 31st, 2009

Jason Ostrom

Arjun Sambamoorthy

Agenda

- Introduction
- Overview of UC
- Live demo of Video Eavesdropping
- Live demo of Video Replay and Video Hijack
- VoIP Pentesting trick
- Conclusion

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Introduction

- **About VIPER Lab**
  - VIPER ~ Voice over IP Exploit Research
  - Security research lab dedicated to finding
    - New UC / VoIP attack vectors
    - Structural vulnerabilities in insecure protocol / deployment / configuration
  - Penetration testing team specialized in VoIP / UC Security
  - Passionate about VoIP / UC Security
  - Replicated a production, enterprise network in VIPER Lab
  - Security assessment professionals supported by research and exploit developers

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Introduction

- **Who we are**
  - Jason
  - Arjun

© 2008 Sipera Systems, Inc. All Rights Reserved.

Sipera Confidential - Do not reproduce or distribute without express written consent

Agenda

- **Introduction**
- **Overview of UC**
  - UC Definition
  - UC Business Cases
  - New UC Attacks
- **Live demo of Video Eavesdropping**
- **Live demo of Video Replay and Video Hijack**
- **VoIP Pentesting trick**
- **Conclusion**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

What is UC?

- **Unified Communications**
  - Voice (VoIP)
  - Video (IP Video)
  - Presence and IM
  - CTI (Computer Telephony Integration) – Desktop Integration
- **Unified Messaging**
  - Voice mail and Email in the same Inbox!

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

The Business Risk

- **Today our presentation will focus on IP Video exploits**
- **Low awareness as to security threats**
  - Security practitioners and IT managers are being pulled into projects to support these new video deployments. But until now, no tools have existed for carrying out testing of IP video vulnerabilities.
- **Video application rollouts as a business driver and ROI**
- **But what about security?**
  - Can an attacker gain privileged access to IP data network through Video infrastructure?
  - How can the IP network be exploited through addition of new video applications?
  - How can the video applications themselves be attacked?

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Real-world Business Examples

- **IP Video**
  - Private IP Video Calling
  - Video Conferencing, or “Telepresence”
- **IP Video Surveillance**
- **Video Streaming Applications**
  - IP TV
- **Others?**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

IP Video Business Case

- **IP Video**
  - Private IP Video calls between individuals
  - IP Video Handsets (hard phones)
  - IP Video soft phone applications
- **Many drivers for enabling the business with increased productivity, cost-savings, and enhanced features**
  - Allows remote workers to communicate “in person”

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Telepresence Business Case

- **Telepresence**
  - HSBC rollout: Saved company US $604,000 in air travel bills

© 2008 Sipera Systems, Inc. All Rights Reserved.

Telepresence Business Case

- **Telepresence**
  - Wachovia: Reduced air travel bills as a result of Telepresence solution

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

IP Video Surveillance Case

- **IP Video Surveillance**
  - IP-based Video Surveillance systems
  - Video Analytics applications
  - Government, Military, Banks, Casinos, Museums

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

IP Video Streaming Applications: Business Case

- **IP Video Streaming Applications**
  - Entertainment venues
  - Professional sports stadiums
- **Real-world examples**
  - "America's Team"

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Cowboys Stadium

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Cowboys Stadium

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Cowboys Stadium

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Cowboys Stadium Details

- **Price Tag: US $1.1 Billion Dollars**
- **Cisco Connected Sports Technologies**
  - Cisco StadiumVision
  - Integrates hi-def video, audio, and digital content into interactive services for fans
  - New revenue streams in advertising with targeted and tailored promotions to HDTV
- **All video traffic carried over IP Network**
- **240 miles of fiber optic cable**
- **2,800 TV Monitors**
  - Each TV Monitor has an IP address
  - Concession stand menus
  - TVs in suites
  - Electronic advertising signs

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Cowboys Stadium Details

- **180 Wireless Access Points**
- **Technology Conference Room, Technology Auditorium**
  - Technology providers can bring their clients to hold meetings and demo products
- **Enough bandwidth to send Hi-Def video from the game to Cowboys Valley Ranch video editing studio, then back to Arlington during halftime. The highlights will be played on the new stadium's video screens.**
- **(2) 60-yard-long HDTV Video boards are largest in the world**
  - Manufactured by Mitsubishi
  - US $40 Million dollar price tag
- **RFID imbedded bracelets for children, so parents can quickly locate them**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Yankee Stadium

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Toronto Blue Jays

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

New UC Attacks

- **Video Replay**
  - Example 1: Video replay against an IP video surveillance system by playing a safe video stream, creating a “blind camera” scenario. Malicious events transpire while human operator can’t see what is really happening.
  - Example 2: An attacker can intercept a live video conference presented by the CEO, and replay the CEO’s previous conference, or a private video session he had with the CFO, in which he told the CFO that they would have layoffs.

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

New UC Attacks

- **IP Video Hijack (Video interception)**
  - A Video interception DoS attack in which we can target a uni-directional RTP video stream, or target specific video endpoints in the middle of a SIP or SCCP video call.
  - Example 1: In the middle of a high-profile sporting event, the attacker can play a random movie clip (including porn).
  - Example 2: In the middle of an important video conference, the attacker intercepts the video stream to play a random movie clip, (including porn).

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

New UC Attacks

- **Video Eavesdropping (Video Recording)**
  - Example 1: Eavesdropping on a private IP video call between the CFO and CEO.
  - Example 2: Eavesdropping on a video conference.
  - Example 3: Re-constructing a safe video stream to play in a loop against a video surveillance camera.

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Agenda

- **Introduction**
- **Overview of UC**
- **Live demo of Video Eavesdropping**
  - Overview
  - Requirements
  - Live Demo: UCSniff Version 3.0
- **Live demo of Video Replay and Video Hijack**
- **VoIP Pentesting trick**
- **Conclusion**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 1.0

- **Released November 2008**
  - Website: http://ucsniff.sourceforge.net
  - Follow UCSniff on Twitter: http://twitter.com/ucsniff
- **First Sniffer software to support new G.722 audio codec**
- **Combined the following features together, to more rapidly test for eavesdropping:**
  - MitM ARP Poisoning
  - Automated VLAN Discovery and VLAN Hop
  - Auto re-construction of forward, reverse media into single WAV file
- **Target Mode**
  - We can intercept and log Skinny keypad messages
  - Theft of voice mail passwords

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 1.0

- **Code design links signaling (SIP, SCCP) and RTP media together**
  - Recording starts via SIP or SCCP message
  - Dynamically adds an RTP dissector when call starts
  - Closes RTP dissector when call ends
- **Result of this Design: We can tell who is calling, not just a random IP address or media stream. I don't like to spend a lot of time looking through media files. We log who and when into the file.**

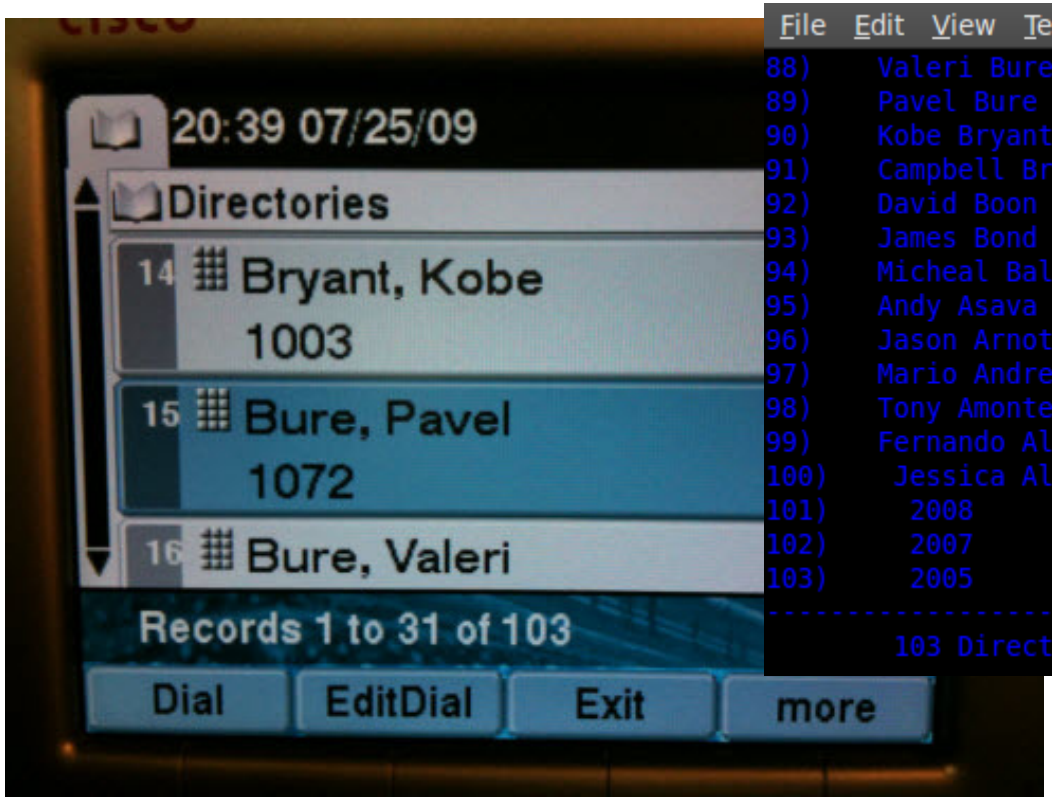
```
Target call ended.  Call duration is 12 seconds.
Saving target user conversation to file, 'Eric Winsborrow_Calling_John (CEO) Rodgers_16:56:8_both.wav'
Target John (CEO) Rodgers (Extension 1004, IP 172.16.96.18) went onhook

Listening for new calls to or from target John (CEO) Rodgers (Extension 1004, IP 172.16.96.18)
```

- **In security testing, time is money; therefore, you have to move fast. UCSniff wraps all necessary features into a single tool.**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 1.0

- **ACE Corporate Directory download feature**
  - Can target VoIP users based on name and extension




```
File  Edit  View  Terminal  Help
88)    Valeri Bure                  1096
89)    Pavel Bure                   1072
90)    Kobe Bryant                  1003
91)    Campbell Brown               1041
92)    David Boon                   1046
93)    James Bond                   1030
94)    Micheal Ballack              1017
95)    Andy Asava                   1000
96)    Jason Arnott                 1088
97)    Mario Andretti               1019
98)    Tony Amonte                  1063
99)    Fernando Alonso              1025
100)    Jessica Alba                 1060
101)     2008                        2008
102)     2007                        2007
103)     2005                        2005
-------------------------------------------------
       103 Directory Users Total
```


© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 2.0

- Released February 2009
- First IP Video Sniffer / IP Video eavesdropping security tool
- Supports H.264 Video Codec

ViperLab

Sipera Systems

© 2008 Sipera Systems, Inc. All Rights Reserved.

Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 2.1

- Released April 2009
- Eavesdropping on Microsoft OCS IM Conversations
- Support for Avaya SIP
- Enhanced ARP Poisoning with Unicast ARP Requests
- Support for G.711 a-law Codec

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 2.1 GARP Research

- Credit: Harsh Kupwade
- We researched the way different IP Phones respond to Gratuitous ARP via the traditional method of unicast ARP reply packets. Successful ARP Poisoning is the basis for the MitM condition.
- Cisco 7985 Video Phones can't be ARP Poisoned unless running UCSniff for 10 minutes. We found a new way: spoofed unicast ARP requests allow immediate ARP Poisoning. 100% effective.
- Avaya IP Phones will not respond to unicast Gratuitous ARP Reply packets (traditional method). Unicast ARP requests are 100% effective, immediately.
- Cisco Unified IP Phones have a "GARP Disabled" security feature. We didn't address this until UCSniff 3.0. We can now bypass it.

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

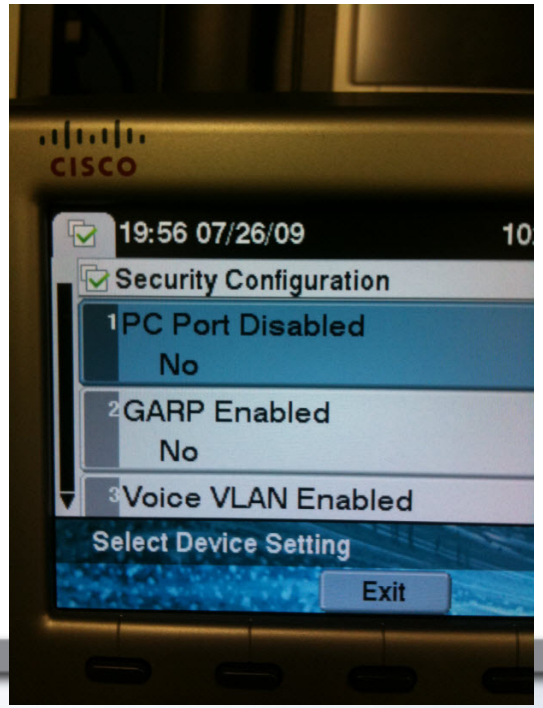
UCSniff 3.0

- **Release August 2009 (tentative)**
- **Creation of GUI using JUCE**
- **Port of UCSniff to Windows OS**
  - Windows VLAN support complete
- **Real time Video Monitor (tentative)**
- **Cisco UCM 7.0 and 7.1 support for Skinny messaging**
- **GARP Disablement Bypass feature**
- **TFTP MitM Feature to modify IP Phone settings**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 3.0 GARP Disabled

- **What is "GARP Disabled"?**
  - A feature in Cisco Unified IP Phones.
  - GARP Disabled is default for all new CUCM installations
  - GARP Disabled means that the IP Phone doesn't populate its ARP cache when an attacker sends spoofed, Unicast ARP Reply packets.



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 3.0 GARP Disabled

- No successful ARP Poisoning = no MitM condition
- With GARP Disabled, we can't ARP Poison the connection from IP Phone → Network. We can, however, ARP Poison the connection from Network → Phone.
- At best, we can only receive ingress RTP media stream from network inbound to IP Phone.

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 3.0 GARP Disabled

- **GARP Disabled is a "Security feature" that is advertised in Cisco best practices, which can defeat a casual attacker to run MitM.**
- **Observations on the way Cisco Unified IP Phones behave with ARP requests when "GARP Disabled" is in effect**
  - When IP Phone boots, sends ARP request to communicate to remote IP gateway, for the traffic communicated to CUCM
  - Doesn't send ARP request for remote RTP peer until it receives SCCP StartMediaTransmission message
- **Winning the "Race Condition"**
  - It is difficult to Poison the ARP request that the phone sends as it boots up, for the IP gateway (to send traffic to remote server)
  - However, during an active call setup, we can predict when the IP Phone will ARP for its remote RTP peer.

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 3.0 GARP Disabled

- **UCSniff 3.0 has a new feature, GARP Disablement Bypass:**
  - ucsniff –i eth0 --garpdb // //
- **The way it works:**
  1. When a call is starting, UCSniff intercepts the 'StartMediaTransmission' message sent from UCM → IP Phone (since we are MitM from network → IP Phone)
  2. UCSniff learns the IP address of both RTP peers. This is how the IP Phone knows who to talk to on the remote end.
  3. UCSniff builds a spoofed unicast ARP reply packet, if the phone is on our source VLAN
  4. We flood the IP Phone with spoofed unicast ARP reply packet
  5. Cisco Unified IP Phone sends an ARP request for valid remote RTP peer
  6. Cisco IP Phone receives spoofed unicast reply packet from UCSniff before it receives the legitimate reply from the valid IP Phone
  7. Flooding continues for a threshold of microseconds after legitimate reply
  8. The IP phone populates its ARP entry with the spoofed entry
  9. UCSniff wins the race condition, ARP Poisoning the IP Phone

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 3.0 GARP Disabled

- **Impact of this**
  - If both IP Phones are in the same VLAN as attacker, we can successfully ARP Poison both IP Phones, and receive bi-directional RTP media
  - If IP Phone is communicating to an RTP peer in remote network, we can still only receive RTP media stream from remote peer inbound to IP Phone

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff 3.0 GUI

- **We used JUCE Libraries to create UCSniff GUI**
  - Website: http://www.rawmaterialsoftware.com
  - "JUCE (Jules' Utility Class Extensions) is an all-encompassing C++ class library for developing cross-platform applications"
  - "It's particularly good for creating highly-specialised user interfaces and for handling graphics and sound."
- **Many props and thanks to Julian Storer**
- **We wanted nice bells, dials, and whistles for video eavesdropping**
- **Very easy to create GUI application using the JUCER & Demo App**
- **We wanted a cross-platform C/C++ application so that UCSniff GUI can look the same way in Mac, Linux, and Windows.**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff Windows Port

- **Porting UCSniff Linux to Windows**
  - MinGW (Minimalist GNU for Windows)
    - http://www.mingw.org/
  - Port of GNU GCC and GNU Binutils for development of native windows applications
- **Creating Voice VLAN interface on Windows**
  - Developed the following two drivers using WinDDK (Windows Driver Development Kit)
    - NDIS protocol driver
    - IM (Intermediate) driver
- **We will release the windows VLAN drivers as a separate package along with UCSniff 3.0**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

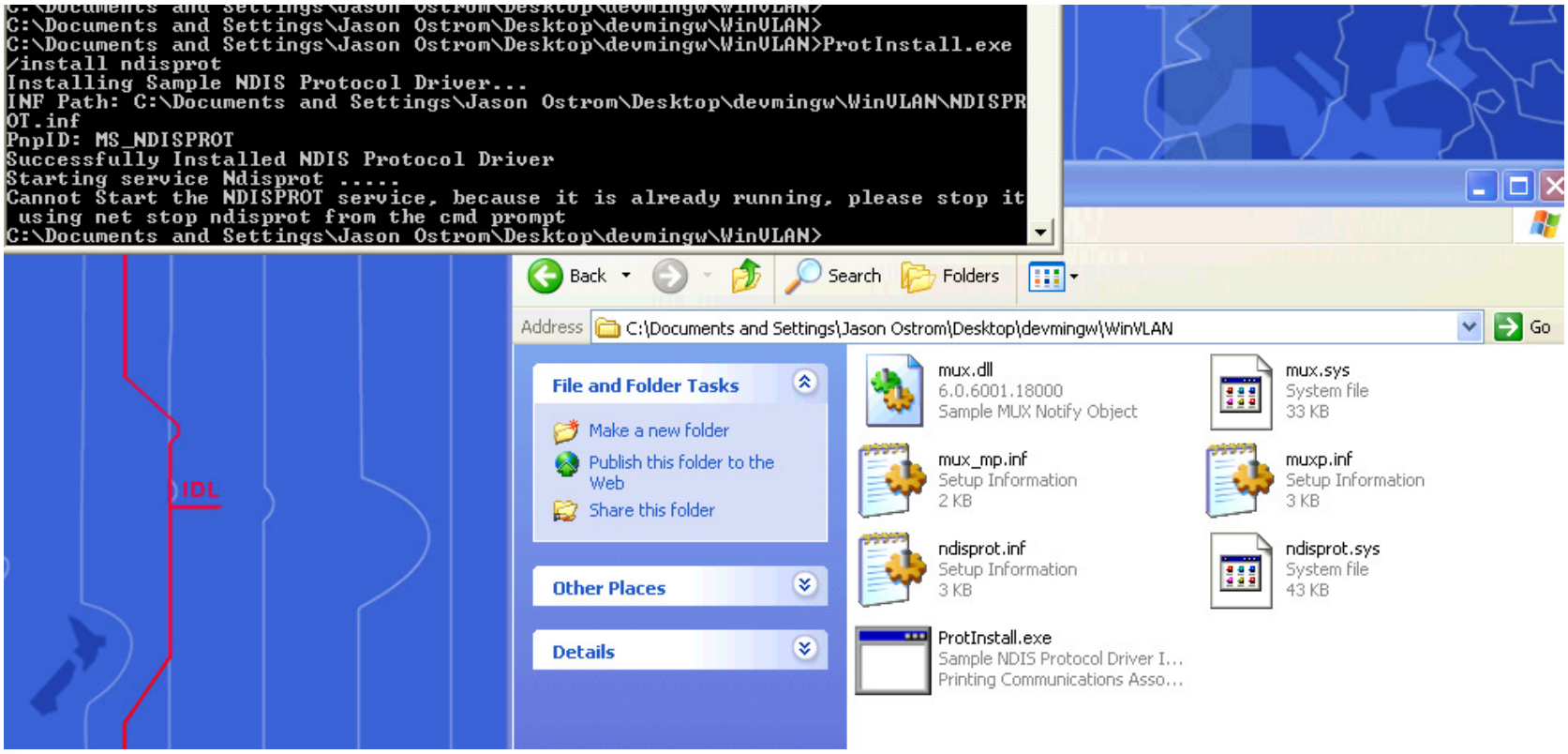
NDIS Protocol Driver

- NDIS (Network Driver Interface Specification) protocol driver, for setting and querying the 8021Q tag on Ethernet interface.
- NDIS protocol driver, to send and receive raw network packets on Windows.

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Installing Ndisprot

- **Using ProtInstall - NDISPROT Driver Installer**
  - http://www.ndis.com/papers/ndisinstall/programinstall.htm



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Starting Ndisprot service

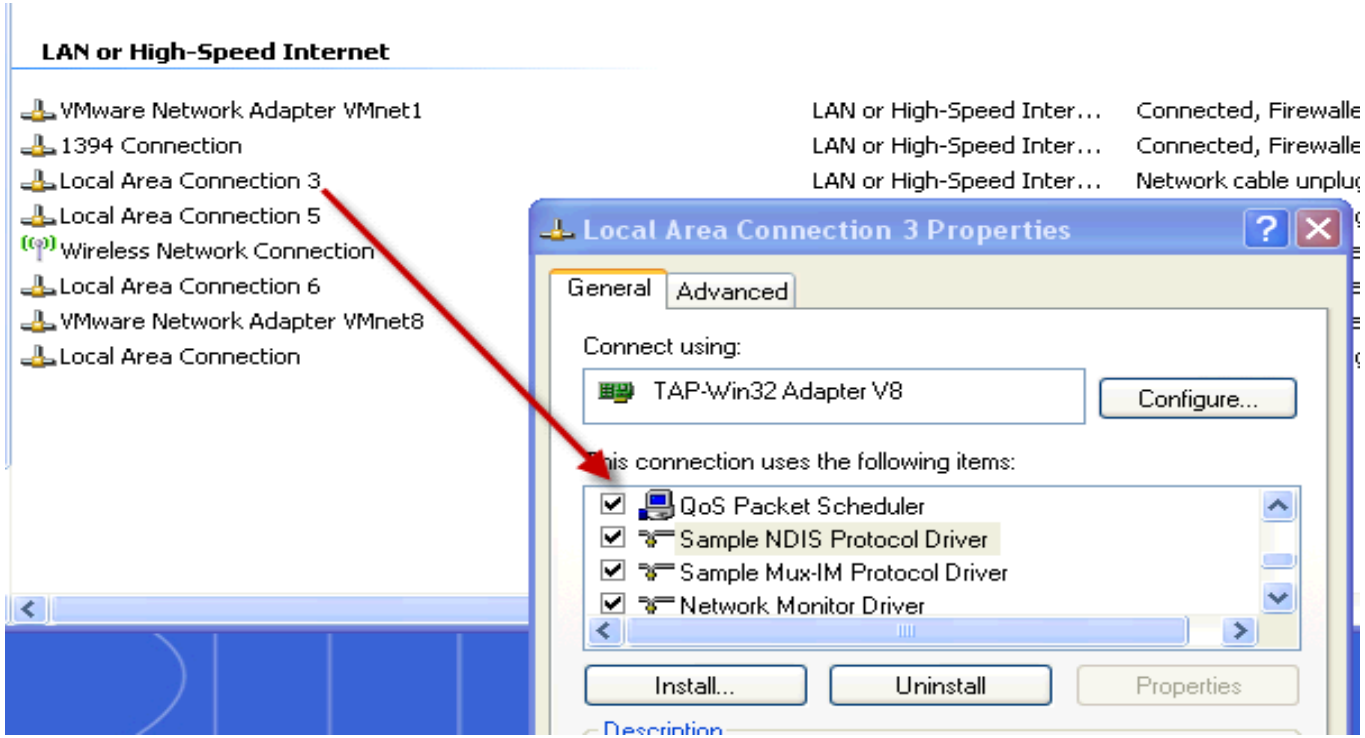
- Execute “net start ndisprot” to start the service
- All these steps will be automated before the official release of UCSniff 3.0

```
C:\Documents and Settings\Jason Ostrom>
C:\Documents and Settings\Jason Ostrom>
C:\Documents and Settings\Jason Ostrom>
C:\Documents and Settings\Jason Ostrom>
C:\Documents and Settings\Jason Ostrom>
C:\Documents and Settings\Jason Ostrom>
C:\Documents and Settings\Jason Ostrom>net start ndisprot

The Sample NDIS Protocol Driver service was started successfully.


C:\Documents and Settings\Jason Ostrom>
```


© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

IM (Intermediate) Driver

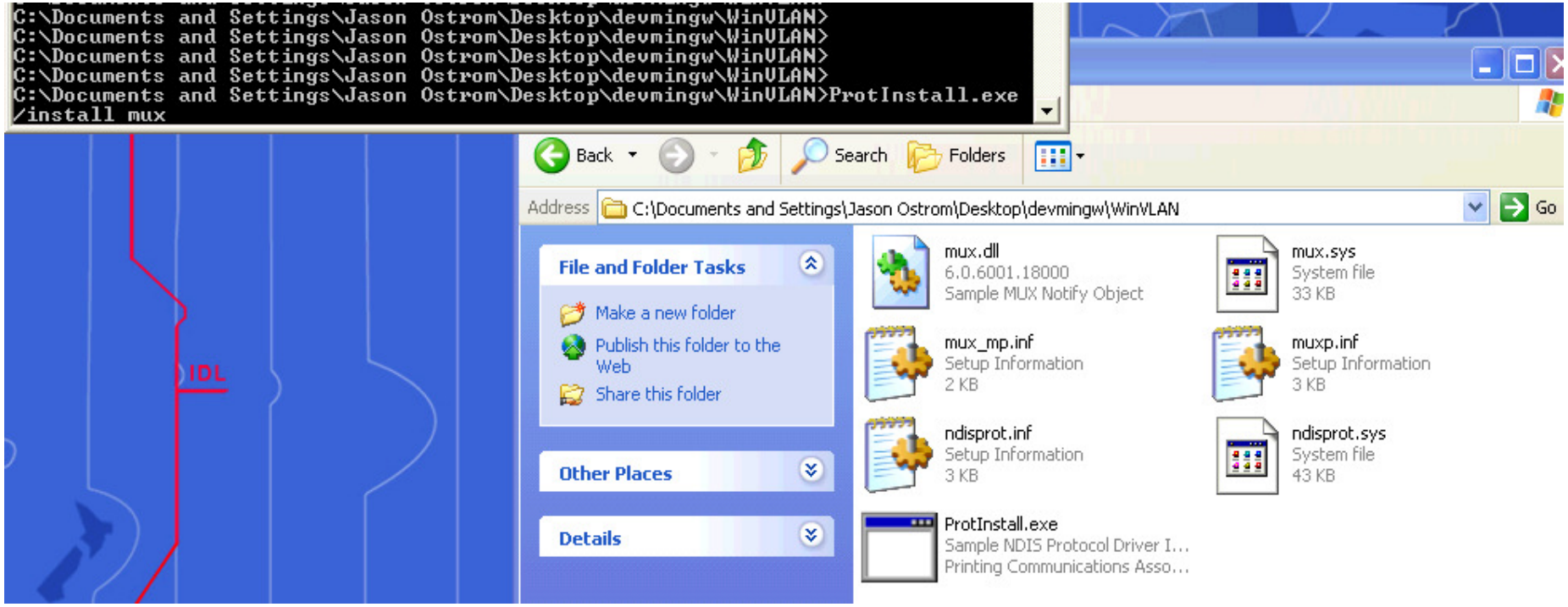
- IM driver creates a virtual interface for both the wired and wireless interfaces
- The virtual interface will be tagged with the Voice VLAN ID



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Installing IM driver

- **Added support for installing/uninstalling IM driver, on NDISPROT Driver Installer (ProtInstall)**



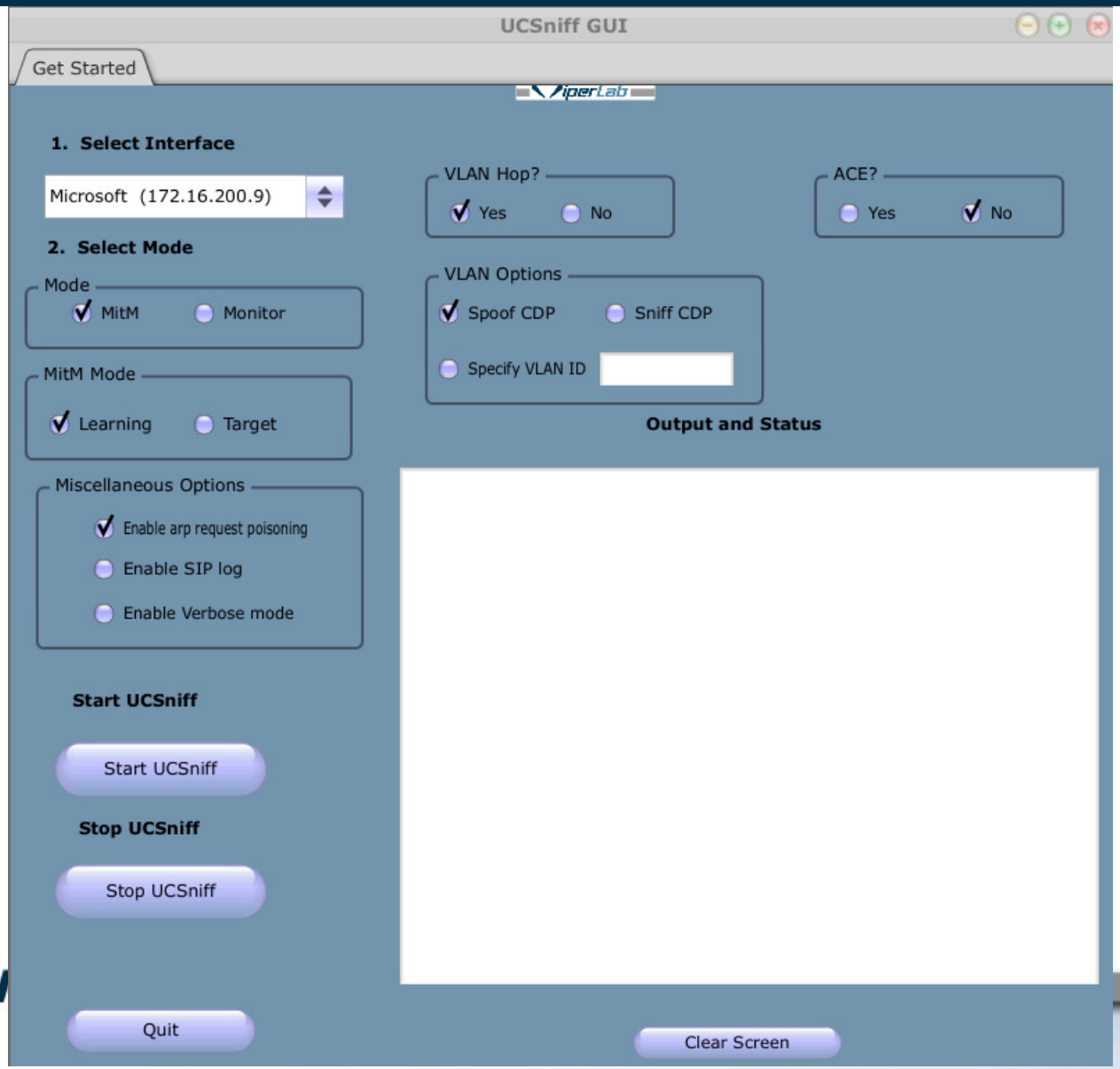
© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Video Decoding Support

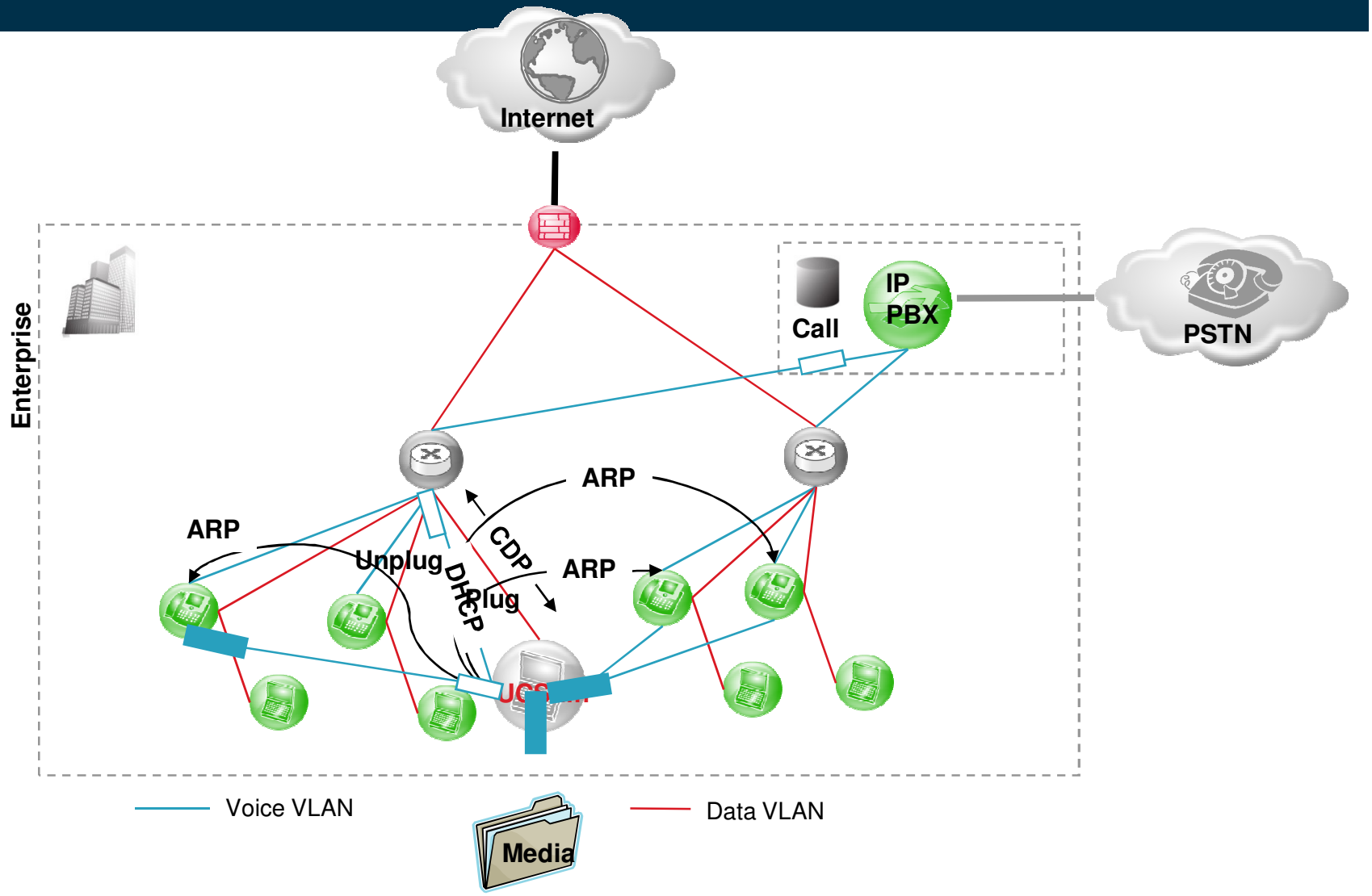
- **Decodes H.264 content from RTP**
- **Compliant with RFC 3984 (RTP payload format for H.264 video codec)**
- **Creates a raw H.264 video only file, playable on VLC and Mplayer**
- **FFMpeg libraries**
  - AVI Container
  - Muxing audio and video

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff Overview



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent



© 2008 Sipera Systems, Inc. All Rights Reserved.

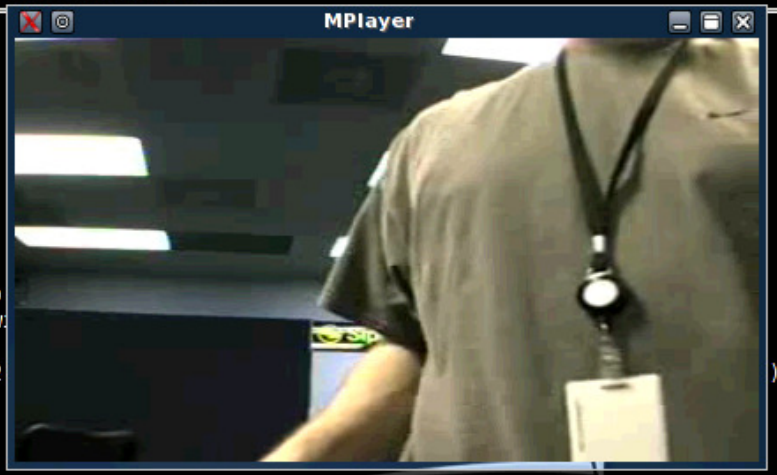
UCSniff Live Demo

- **Targets: (2) Cisco 7985 Video phones**

Shell - Konsole <2>

```
4 hosts saved to arpsaver.txt

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)

Starting Unified sniffing...

Warning:  Please ensure that you hit 'q' when you are finished with this p
Warning:  'q' re-ARPs the victims.  Failure to do so before program exit w

Call 1 (SCCP) in progress at 15:33:7. 'Mike Jones (CEO)' (Number 1069, 172
172.16.100.1 --> 172.16.99.5: OpenMultiMediaChannelMessage
172.16.99.5 --> 172.16.100.1: OpenMultiMediaReceiveChannelAckMessage
172.16.100.1 --> 172.16.99.4: OpenMultiMediaChannelMessage
172.16.99.4 --> 172.16.100.1: OpenMultiMediaReceiveChannelAckMessage
Saving forward video conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_forward_video.avi'
Saving reverse video conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_reverse_video.avi'
Saving audio conversation to file, 'Mike Jones (CEO)_Calling_Sara Jones (CFO)_15:33:7_both.wav'
Call 1 (SCCP) ended at 15:33:16.  Call duration is 9 seconds.
```

MPlayer



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Agenda

- **Introduction**
- **Overview of UC**
- **Live demo of Video Eavesdropping**
- **Live demo of Video Replay and Video Hijack**
  - Overview
  - Requirements
  - VideoJak Live Demo
- **VoIP Pentesting trick**
- **Conclusion**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

VideoJak 1.0 – HiJacking IP Video

- **Released February 2009 ~ Credit: Abhijeet Hatekar, Author**
  - Website: http://videojak.sourceforge.net
  - Follow VideoJak on Twitter: http://twitter.com/videojak
- **First security assessment tool to support H.264 video codec**
- **First version can run a targeted DoS against an IP video conversation using Cisco 7985 IP Phones**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

VideoJak 1.1

- **Will be released August 2009 (tentative)**
- **New features:**
  - Video Replay in a continuous loop, using AVI file
  - Video DoS attack against a video endpoint, using AVI file
  - Can replay a previous IP video call conversation using raw H.264 container

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

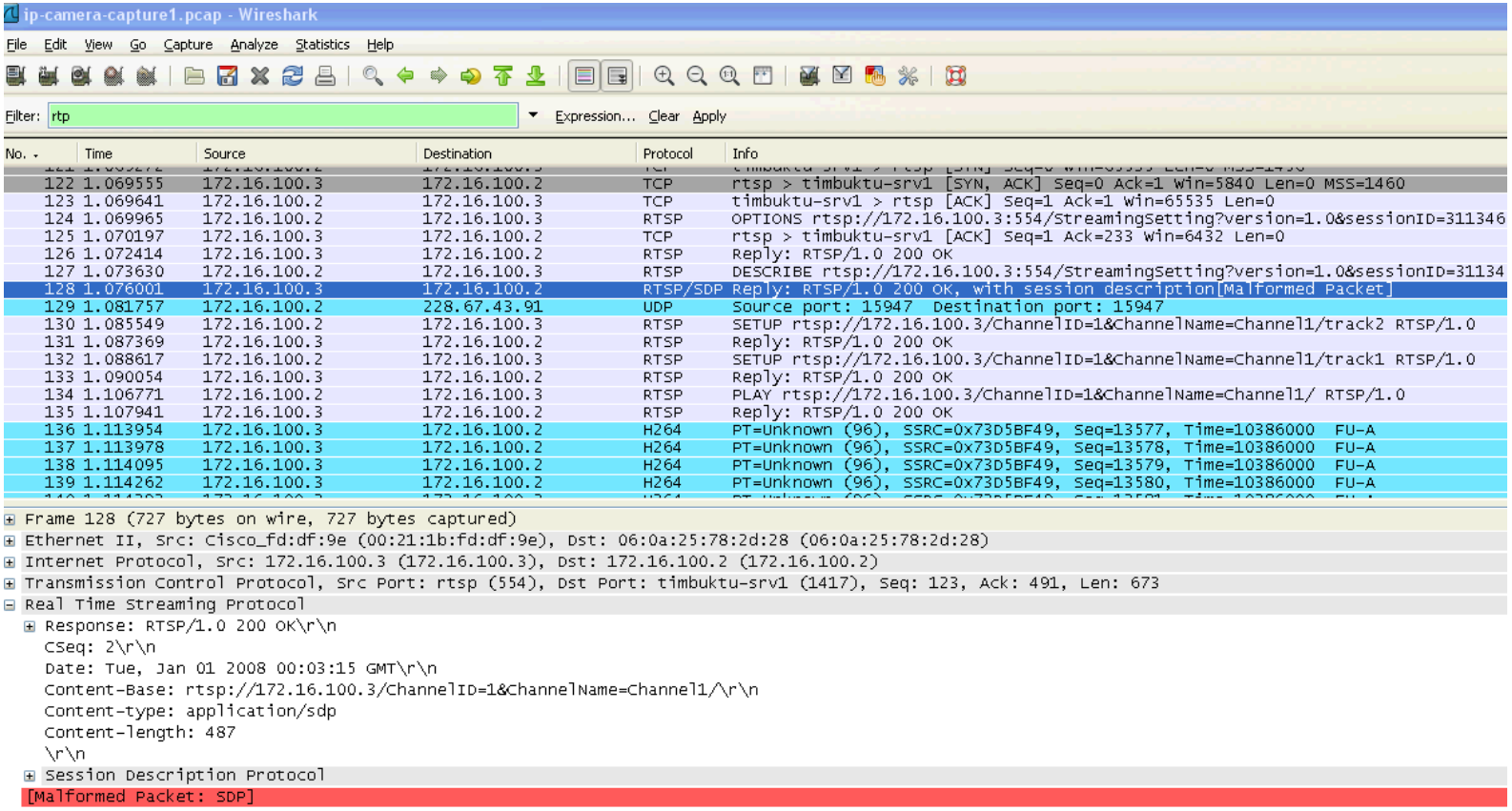
VideoJak Development

- **Finding a valid H.264 RTP stream**
  - Easy to find an H.264 RTP stream, if we can intercept the signaling (SIP/Skinny/RTSP/SDP) that negotiates the RTP port and other codec parameters.
  - Signaling and session negotiation takes place only once and it does not happen very frequently.
  - Particularly, in case of IP video surveillance, media could be streamed to the monitoring end point for days without any signaling.
  - We came up with a module to intelligently detect an RTP stream based on the:
    - IP and UDP parameters
    - RTP Version
    - Payload Type
    - SSRC
    - Monotonically increasing sequence number and timestamp

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

VideoJak Development

- **Sample capture showing a session getting established between IP video surveillance camera and a monitoring end point.**



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

VideoJak Development

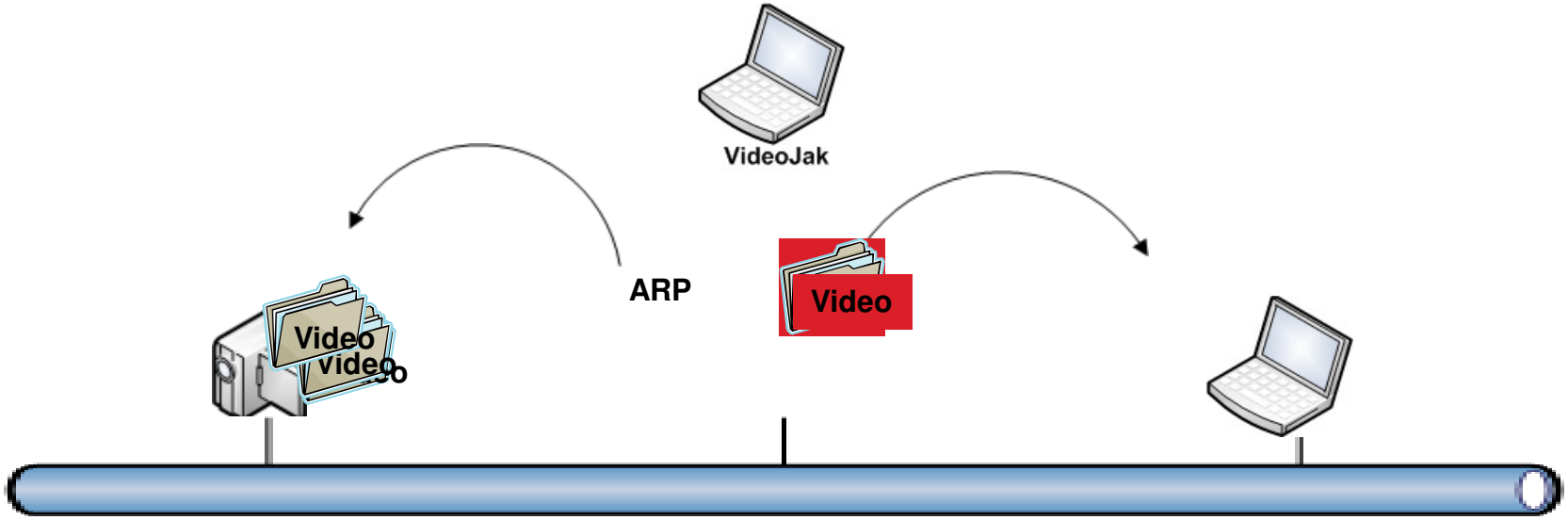
- **H.264 payload format and fragmentation**
  - Four types of H.264 RTP payload formats. (Single NALU, FU, STAP, MTAP)
  - If the H.264 payload size exceeds the MTU, the payload gets fragmented at the H.264 level . These H.264 format are called FU-A or FU-B.
  - Some H.264 clients like Cisco 7985 don't handle FU-A or FU-B H.264 payload formats.
  - For Cisco 7985 phones, VideoJak automatically converts FU type payload to Single NALU payload type and fragments them at the IP level.
- **FFMpeg libraries**
  - To convert the AVI and raw H.264 file to RTP media stream
  - The converted RTP media stream headers are initialized with the:
    - Original RTP stream's SSRC
    - Payload Type
    - Incremented sequence and timestamp values
    - Spoofed source IP and UDP port of valid video sender

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

VideoJak Overview

- **Target an H.264 RTP Video stream**
  - Select the 1-way video stream
  - Start attack, by dropping the valid RTP packets
- **Video DoS Exploit**
  - Select the AVI or H.264 raw file
  - Use Libnet to construct the H.264 RTP packet
  - Use SSRC, timestamp, and other values of dropped packet
  - Video interception can be a replay or random movie clip
  - Target video device and send AVI file on destination RTP port

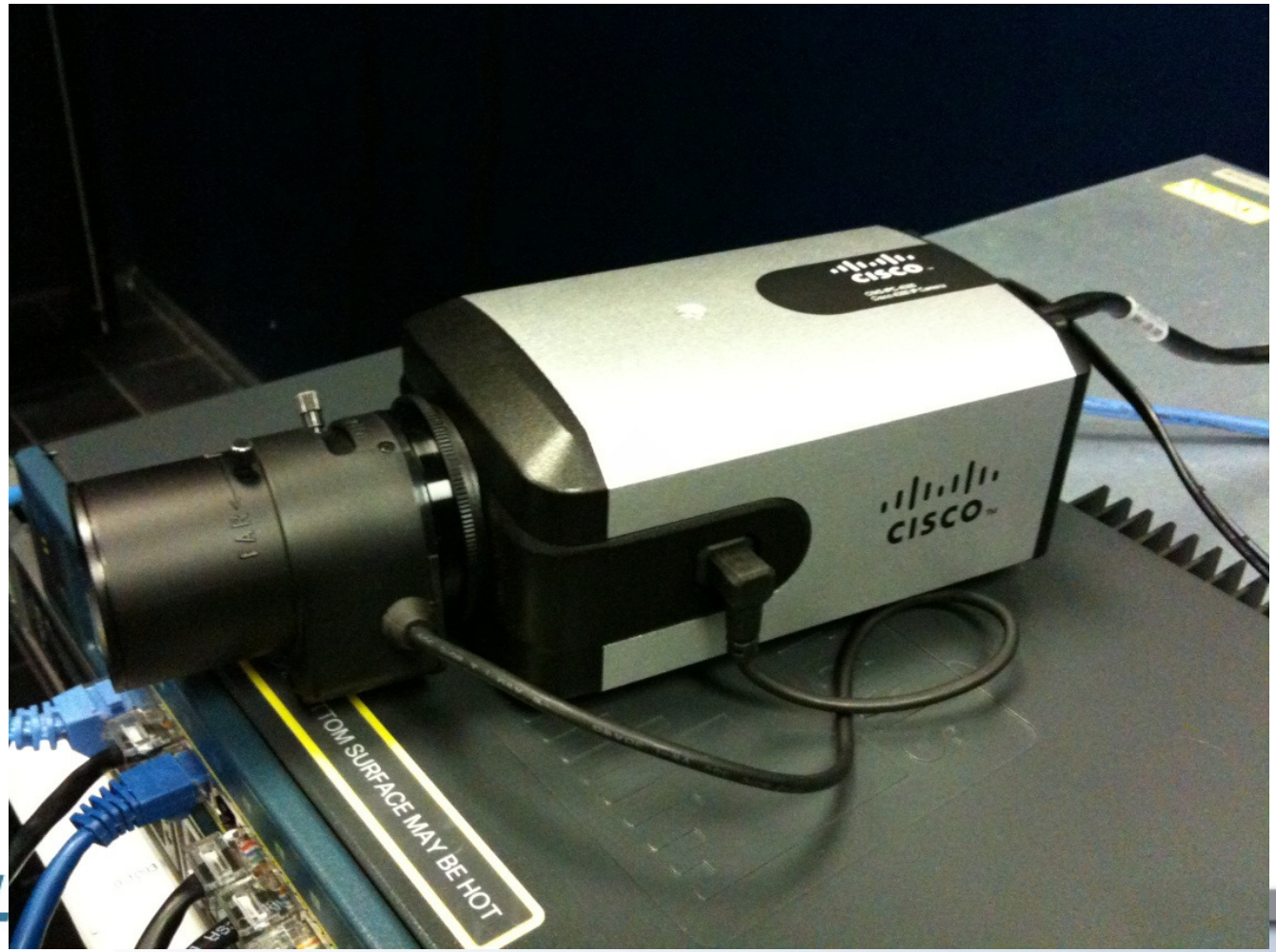
© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent



© 2008 Sipera Systems, Inc. All Rights Reserved.

VideoJak Target

Cisco 4300 Series IP Camera



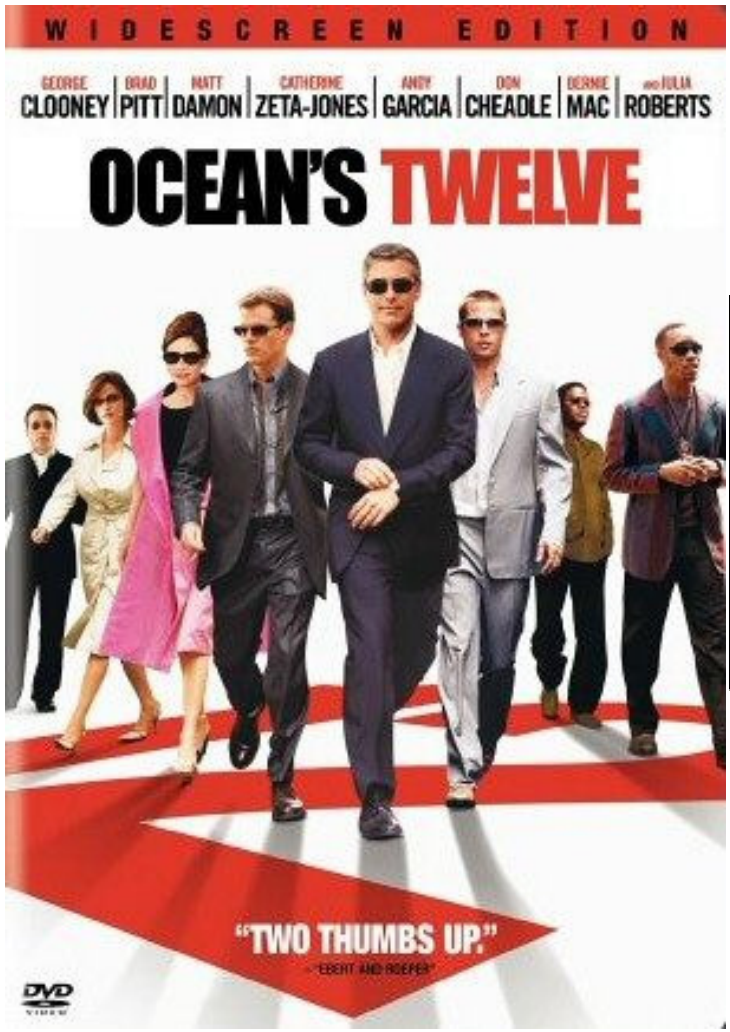
© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

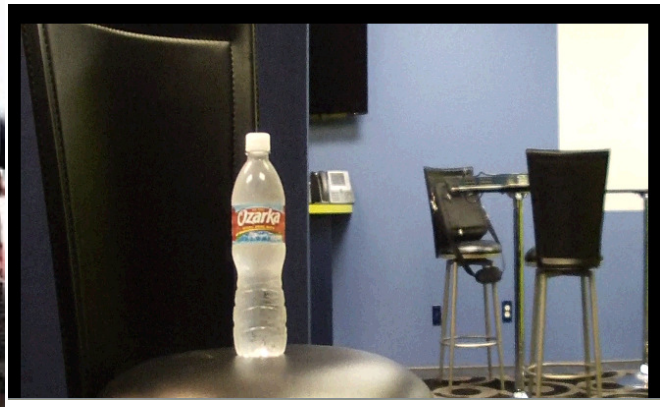
VideoJak Targets

- **Cisco 4300 Series IP Camera**
  - Cisco “Physical Security” solutions portfolio
  - 1080p High Definition (HD) Video
  - Uses RTP to stream H.264 compressed frames
  - Uses RTSP for port negotiation
  - Supports security features such as SRTP and 802.1x
  - 10/100 FE with PoE, or wireless
  - Web application (Active X control) for remote viewing from PC
  - Video Analytics: 4500 series supports DSP-based, programmable
- **Purchased from Cisco reseller specializing in Video surveillance**
  - EYESthere → http://www.eyestheredfw.com
- **For this demo, we will target the uni-directional RTP stream from the IP camera to our demo laptop.**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

VideoJak Tool Demo





© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Agenda

- **Introduction**
- **Overview of UC**
- **Live demo of Video Eavesdropping**
- **Live demo of Video Replay and Video Hijack**
- **VoIP Pentesting Tricks**
  - Stealth Target Mode
  - Story of modify IP Phone settings
- **Conclusion**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

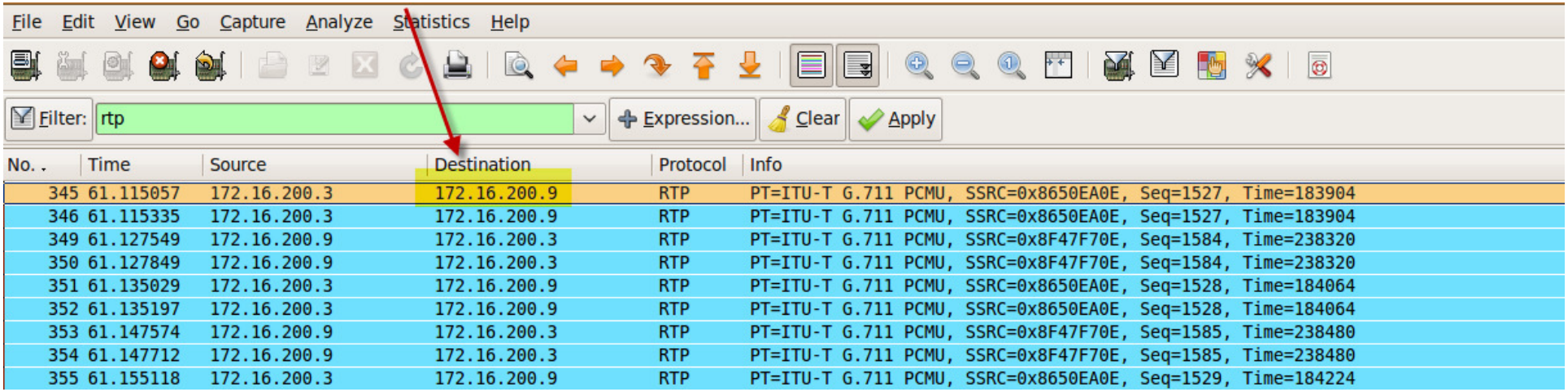
The Ultimate UCSniff Trick

- **This is the ultimate stealth UCSniff trick that can have you eavesdropping a targeted user with the least risk of service impact.**
  - So smooth and stealth, even a Ninja would be impressed
- **First, you need to know the IP address of target IP Phone. If you know the IP address, skip this step.**
- **You don't have to ARP Poison all of the traffic.**
- **You don't have to walk into the cube of the targeted user and look at their phone, learning the MAC Address of the IP Phone.**
- **There is a clandestine way to learn this information remotely.**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Find IP Address of remote IP Phone

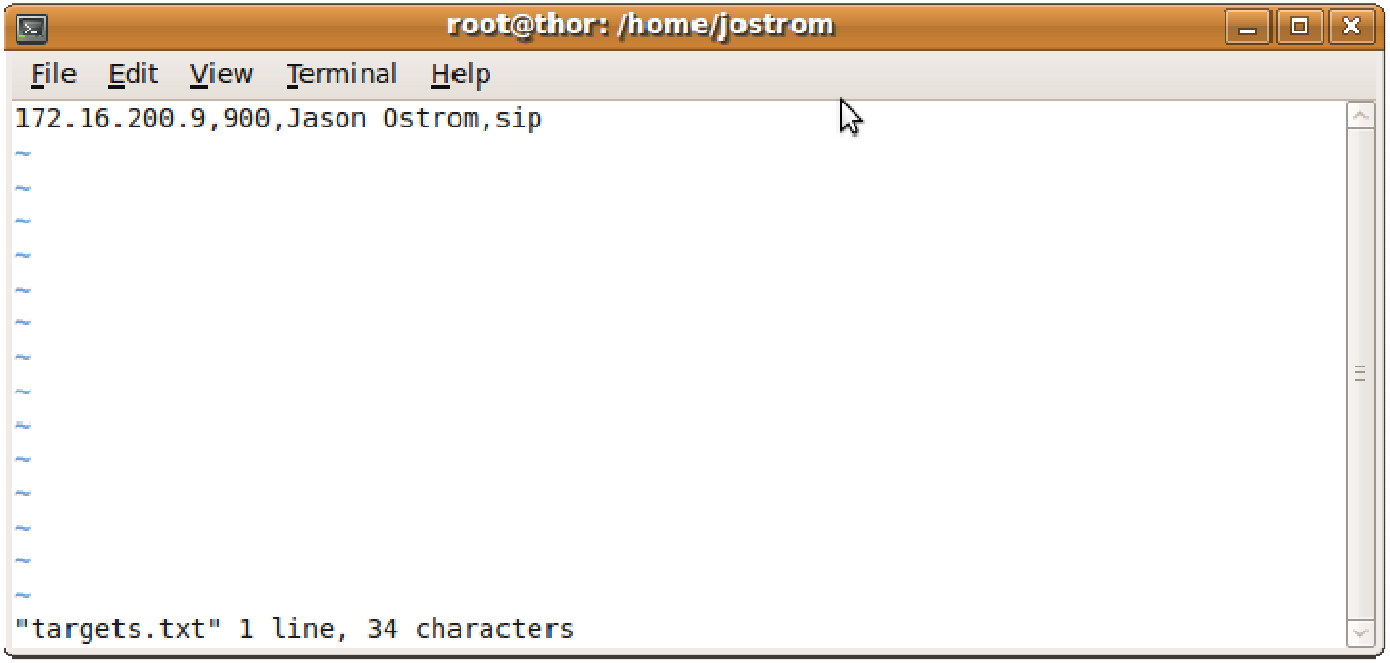
- **To clandestinely find the IP address of remote IP Phone:**
  - Share a hub with laptop and IP Phone
  - Sniff traffic with Wireshark
  - Call remote User (Via corporate directory, Intranet)
  - Remote called party must pick up – Remote Phone must go offhook
  - Decode RTP Packets to find remote IP address
  - Wireshark RTP filter will find IP address



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Create Targets Entry

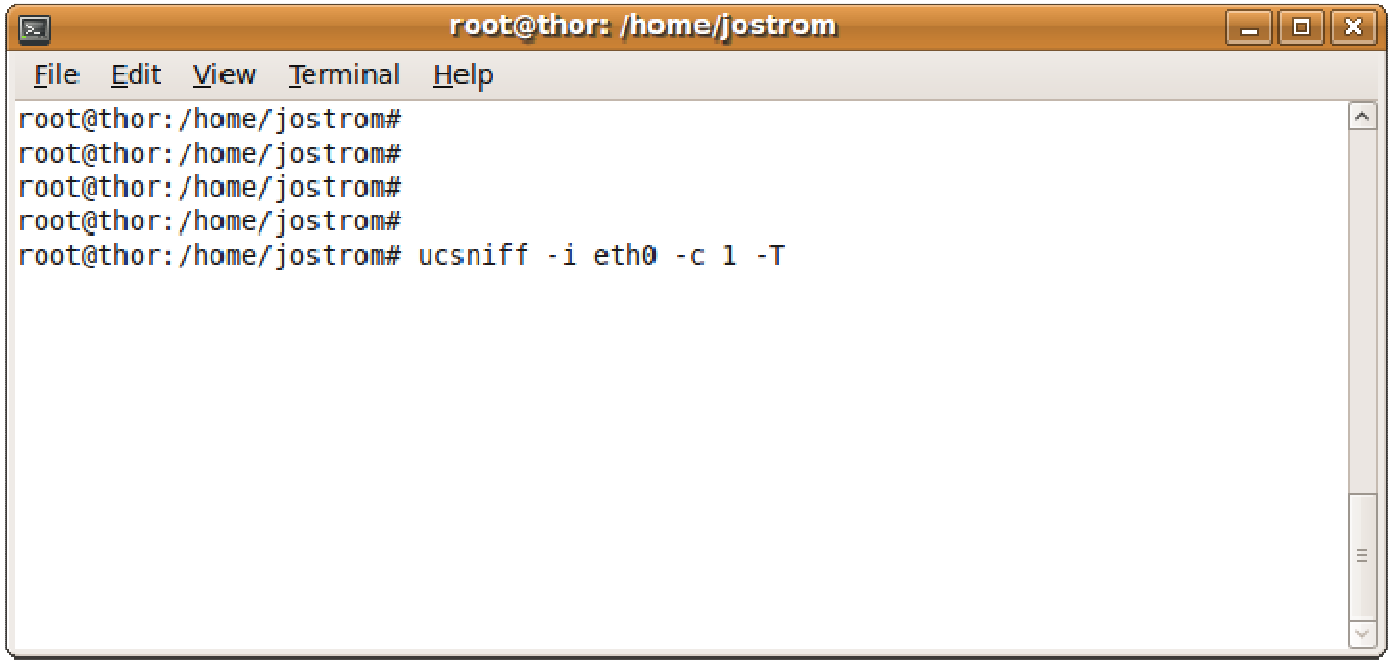
- **Manually create file targets.txt**
  - Manually create file targets.txt, including IP address of discovered remote IP Phone target



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff Target Mode

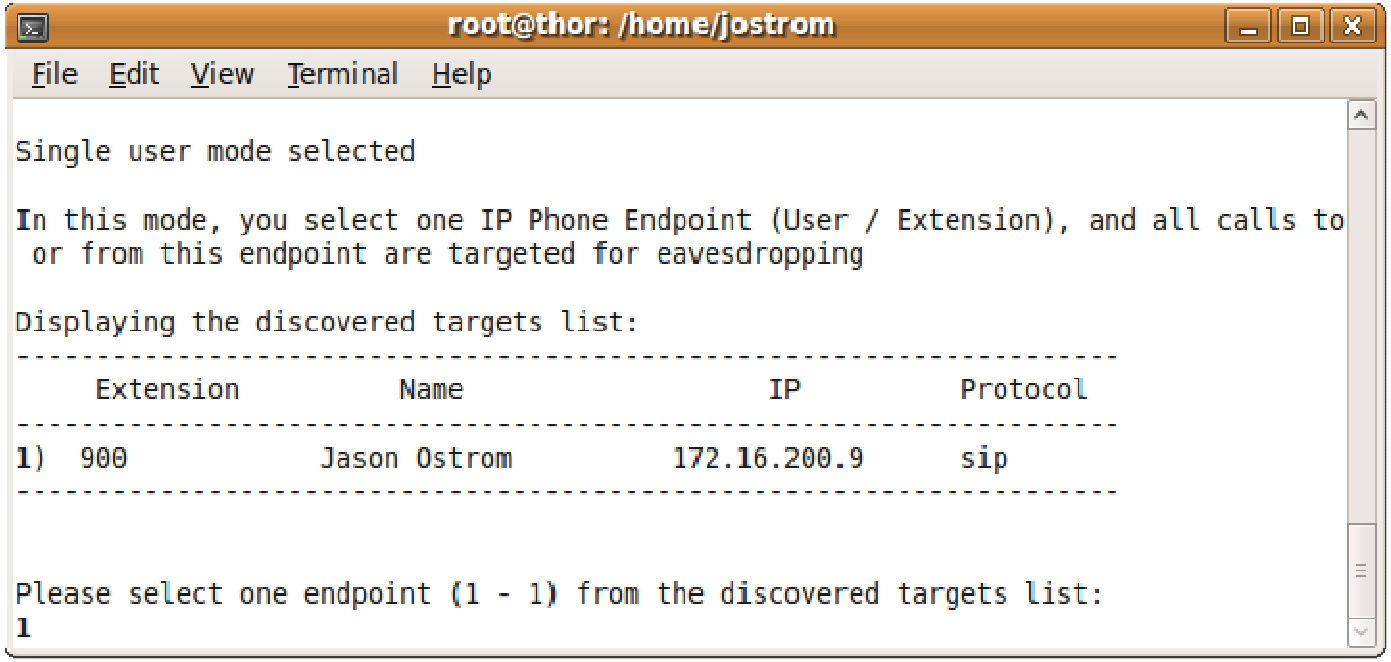
- **Run UCSniff in targeted user mode**
  - Usually 'ucsniff –i eth0 –c 1 –T'
  - Select Option 1 for Single User Mode



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Select Targeted User

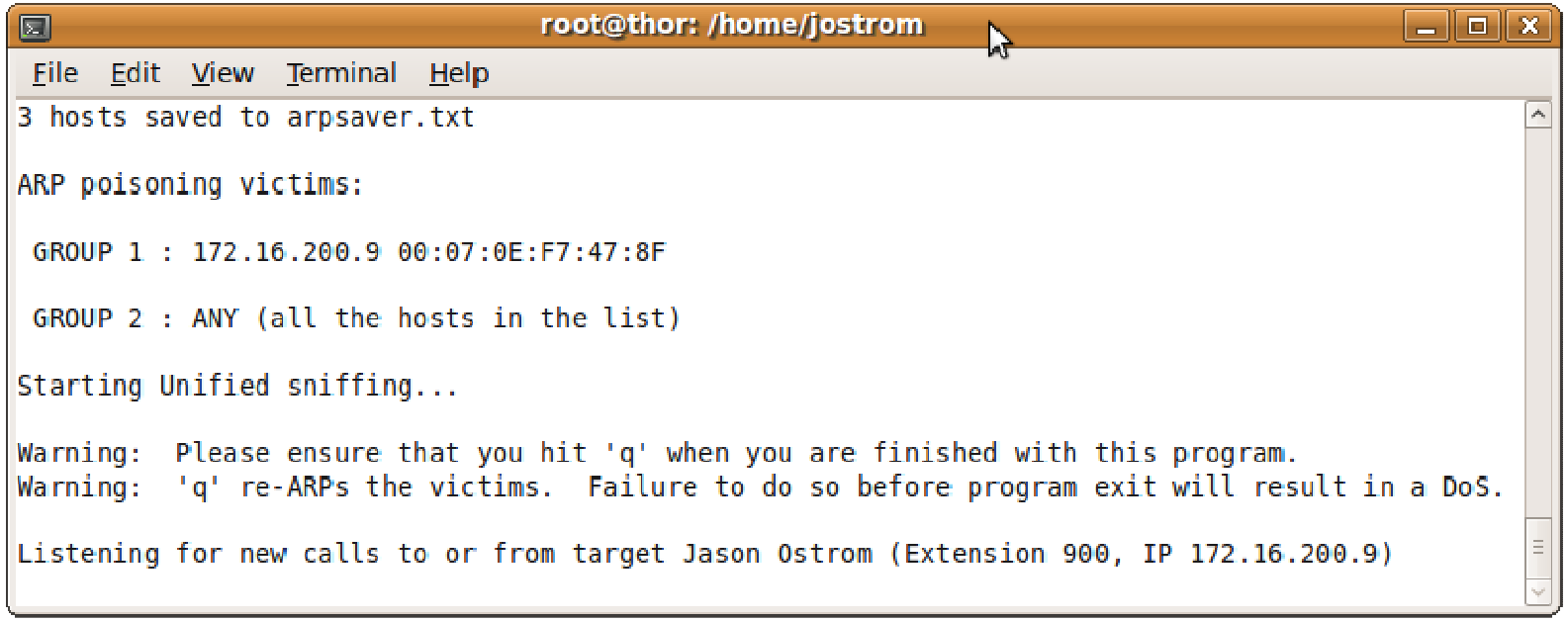
- **Select targeted user**



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

UCSniff Stealth Mode Targeted Eavesdropping

- **UCSniff is now intercepting the traffic of only the targeted user's IP Phone. All calls to or from this user will be recorded.**
  - Low risk of impact
  - Will not impact other IP Phone users



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

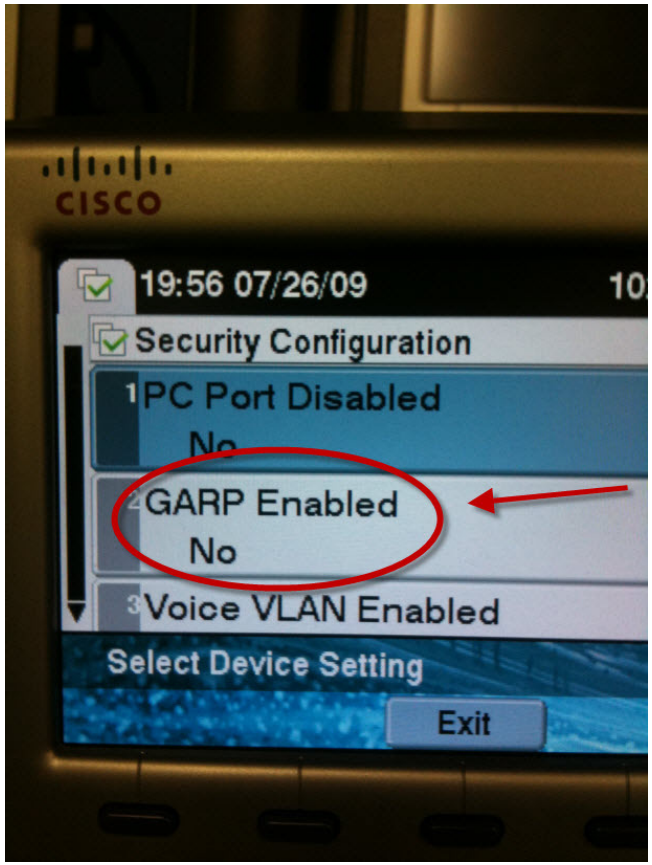
Background of a Live UC Pentest

- VIPER Security Consultant onsite with client in Europe
- Authorized penetration test against Cisco UCM 7.1 VoIP environment
- By default, GARP was disabled on all Cisco Unified IP Phones
- For IP Phones calling each other in same VLAN, we could re-construct RTP media with –garpdb feature of ucsniff
- For IP Phones calling to remote VLANs, we could only re-construct traffic in ingress direction due to “GARP disabled”
- We couldn’t intercept Skinny keypad messages for theft of voice mail passwords (as we could do before)

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Background of a Live UC Pentest

- **The "GARP Disabled" feature was getting in the way of a very successful pentest**



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Background of a Live UC Pentest

- **We had to figure a way to remotely Enable GARP on the IP Phone**
- **We knew that:**
  - "GARP Enabled" is a setting that is managed via the server, by specifying the configuration for that IP Phone
  - Cisco Unified IP Phones download the configuration file via TFTP, which tells the IP Phone how to configure itself
- **This configuration file is only downloaded when the Phone boots up and registers via Skinny / SCCP protocol**
- **Could there be a way for us to force the IP Phone to download this configuration file, and somehow modify it?**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Background of a Live UC Pentest

- We figured out a method to do this via an automated process
- We wrote a new feature of UCSniff that can remotely change the configuration of an IP Phone, thus enabling GARP
- This is done through the MitM engine of UCSniff, and we've called it "TFTP MitM IP Phone modification" vector
- This new feature will be included in UCSniff 3.0
- In the following screen shots, UCSniff will step through the required methods
- Note: This method can be mitigated by applying security controls to a default installation

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Prepare UCSniff

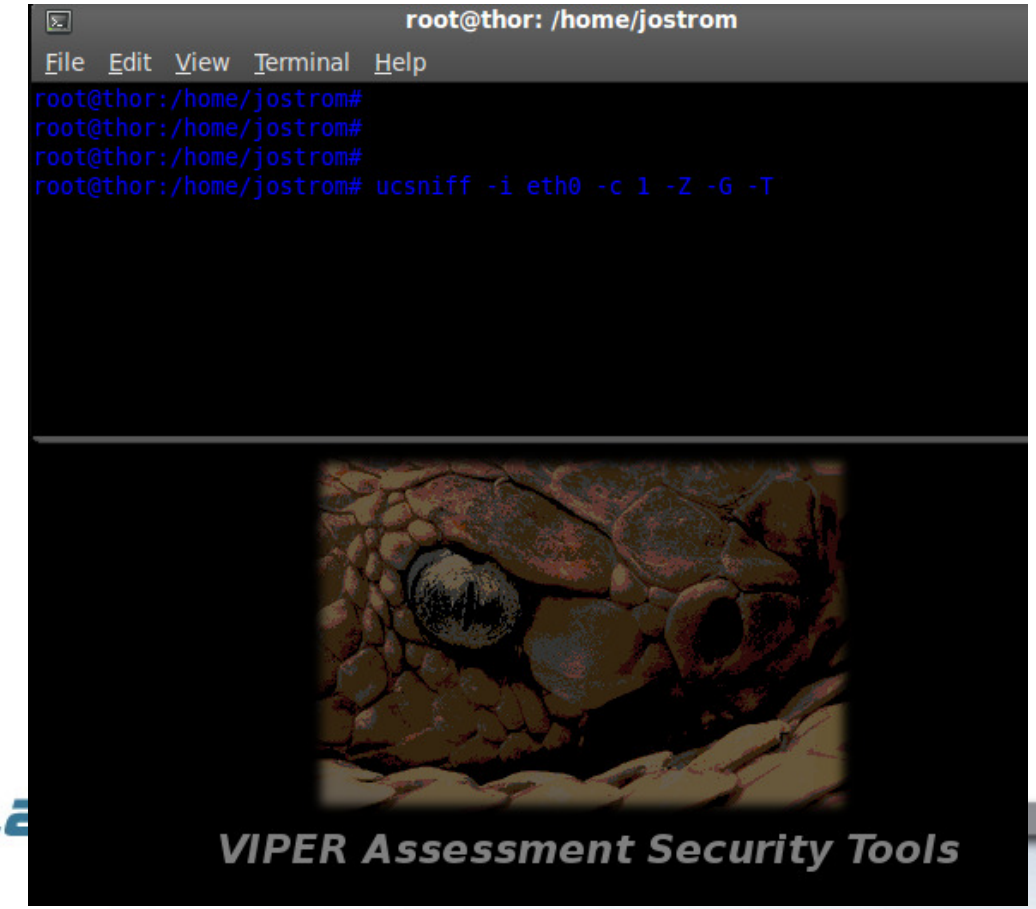
- We must first have physical access to port that is a member of the Voice VLAN for the IP Phone we want to change (MitM Condition)
- We should know the IP address for that IP Phone

First, create the targets.txt file with the IP address of the IP Phone

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Launch UCSniff with new feature

- **Launch UCSniff with new feature:**
  - ucsniff –i eth0 –Z –G –T
  - This can only run in Target Mode, against a single IP Phone



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Step 1: Drop KeepAliveAckMessage

- Cisco SCCP IP Phones use a KeepAlive/KeepAliveAckMessage as a heartbeat mechanism, letting the IP Phone know it has a connection to the server
- The KeepaliveAckMessage is the response message sent from CUCM to the IP Phone
- Since we are MitM for any traffic from Network → IP Phone, we can drop this message
- UCSniff drops the KeepAliveAck Message from the server → IP Phone

```
Listening for new calls to or from target Jason (Extension 1020, IP 172.16.99.47)
Dropping KeepAliveAckMessage:  172.16.100.1 --> 172.16.99.47
Dropping KeepAliveAckMessage:  172.16.100.1 --> 172.16.99.47
Dropping KeepAliveAckMessage:  172.16.100.1 --> 172.16.99.47
Dropping KeepAliveAckMessage:  172.16.100.1 --> 172.16.99.47
```


© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

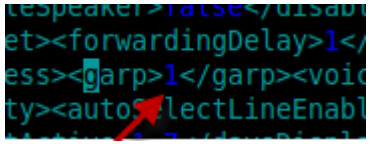
Step 2: IP Phone Registers, downloads Configuration file

- Since the IP Phone believes it has lost connectivity to the server, it attempts to Register to CUCM
- When the IP Phone registers, it downloads the configuration file via TFTP
- We intercept the served TFTP file via a UDP stream dissector in UCSniff
- UDP stream destined to IP Phone is dissected. We look for the GARP setting within the UDP Stream

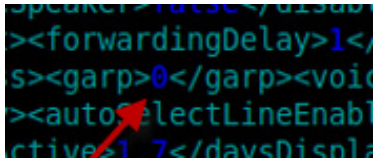
© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

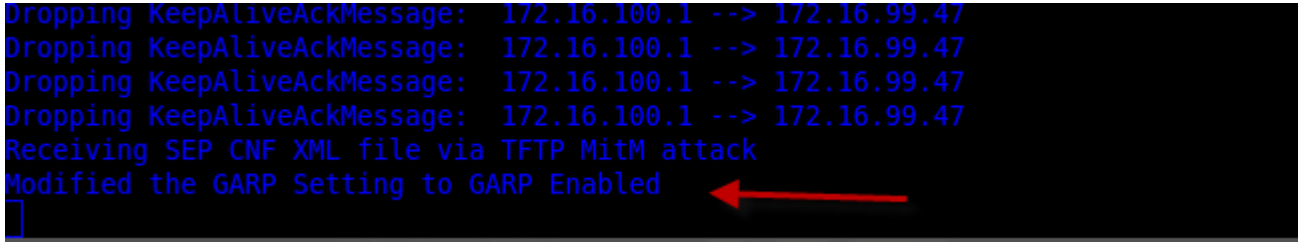
Step 3: Modify configuration setting for GARP via UDP Stream

- GARP Setting is changed over the network, from “GARP Disabled”



- To “GARP Enabled”

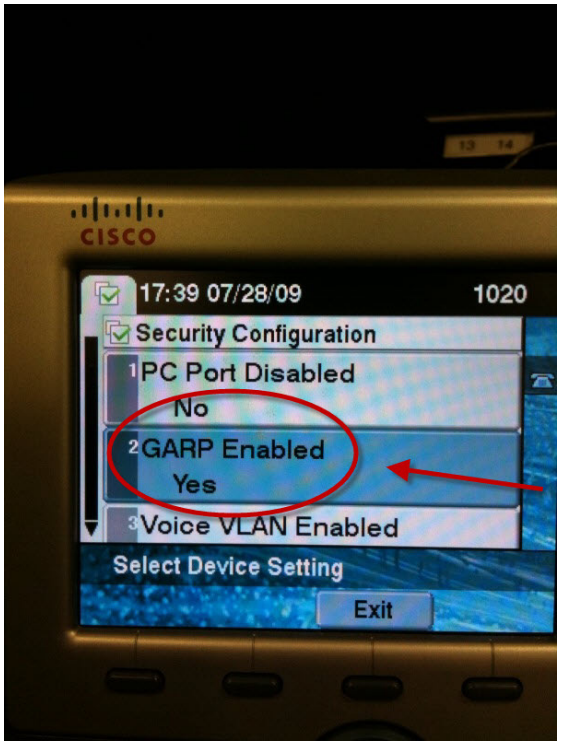




© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Step 4: Cisco IP Phone parses new configuration

- Cisco IP Phone finishes download of Configuration file via TFTP
- Cisco IP Phone parses new configuration, Enabling GARP



© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Summary

- **This happens in less than 30 seconds**
  - IP Phone will keep settings until it is rebooted
- **IP Phone will blank out when it loses registration for ~ 20 seconds**
  - If user is watching their IP Phone LCD, they might see the blankout and lost registration
- **Pentest Trick**
  - Wait until employees go home for the day
  - Target each IP Phone, Enabling GARP
  - When employees arrive for work the next morning, they can be targeted for VoIP / Voicemail eavesdropping

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Summary

- **We can modify any IP Phone setting that is controlled by SEP Configuration file**
  - We could add new features and modules for modification of IP Phone configuration
- **In the absence of security controls, all Cisco Unified IP Phones are vulnerable to this issue with UCSniff 3.0**
- **As stated before, this can be mitigated by following Cisco Security Best practices**
  - See the Cisco SAFE Architecture
  - http://www.cisco.com/en/US/netsol/ns954/index.html

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent

Contact Information

- **Jason Ostrom, CCIE #15239 Security**
  - Director, VIPER (Voice over IP Exploit Research)
  - jostrom@viperlab.net; iknowjason@pobox.com
- **Arjun Sambamoorthy**
  - Research Engineer
  - arjun@viperlab.net; arjunsam@gmail.com
- **For more information about Sipera VIPER Lab, visit us online at http://www.viperlab.net**
- **For more information about Sipera Systems, visit us online at http://www.sipera.com**

© 2008 Sipera Systems, Inc. All Rights Reserved.
Sipera Confidential - Do not reproduce or distribute without express written consent