



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**



Sipera Systems

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



Sipera Systems

Introduction

- Who we are

- Jason
- Arjun



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**



Sipera Systems

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!



Sipera Systems

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?



Sipera Systems

Real-world Business Examples

➤ IP Video

- Private IP Video Calling
- Video Conferencing, or “Telepresence”

➤ IP Video Surveillance

➤ Video Streaming Applications

- IP TV

➤ Others?



Sipera Systems

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”



Sipera Systems

Telepresence Business Case

➤ Telepresence

➤ HSBC rollout: Saved company US \$604,000 in air travel bills

The screenshot shows a web browser window with the following details:

- Title Bar:** HSBC begins global TelePre... (partially visible)
- Address Bar:** http://www.zdnetasia.com/news/communications/0,39044192,62045927,00.htm
- Toolbar:** Customize Links, Windows, Report a Security Vul..., C++ Beginner's Guide, Testing SIP Security o..., Skype for SIP Beta - ..., Skype For SIP now av..., GNU 'make'
- User Options:** Log in | Sign up | Members' privileges
- Content Area:**
 - ZDNet Asia Logo:** Where Technology Means Business
 - Advertisement:** SYMANTEC IS STORAGE SOFTWARE.
 - Article Headline:** HSBC begins global TelePresence rollout
 - Article Subtext:** By Nick Heath, Special to ZDNet Asia | Tuesday, September 09, 2008 10:27 AM
 - Text Content:** HSBC is on course to make big savings and slash its air travel by millions of miles as it begins a global rollout of Cisco's videoconferencing system, TelePresence. The system has already proven successful for HSBC: during one month of use between its 8,000-strong London HQ and its Hong Kong office, the bank saved US\$604,000 on air travel bills and reduced distance flown by staff by 522,000 miles.
 - Related News:** SMBs in S'pore, India to spend US\$1B on Net; Cisco buys e-mail provider PostPath; Cisco invests in the future; Cisco acquires video management start-up; Cisco revamps enterprise mobility architecture
 - Symantec Advertisement:** Symantec Storage Solutions STOP BUYING STORAGE
 - Hot Spot:** What's important from our sponsors
 - Accenture Advertisement:** Join Accenture

Telepresence Business Case

➤ Telepresence

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

The screenshot shows a web browser window with the URL <http://www.networkworld.com/community/node/15874>. The page is titled "DEMAND MORE RETURN ON INNOVATION" and features the "NETWORKWORLD" logo. The main content is an article by Brad Reese titled "Wachovia Securities to slash costs with Cisco TelePresence". The article discusses how Wachovia is using Cisco TelePresence 3000 systems to connect its Richmond, VA headquarters with its Charlotte, NC parent bank, thereby reducing air travel costs. A quote from Jim Kittridge, Wachovia Senior IT Leader and Telepresence product manager, is included. The page also includes social sharing options (Share, Tweet This, Email this page, Comment, Print) and a newsletter sign-up button. A Microsoft Virtualization advertisement is visible on the right side of the page.

IP Video Surveillance Case

➤ IP Video Surveillance

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

The screenshot shows a web browser window with the URL <http://www.networkworld.com/news/tech/2009/062209-tech-update.html>. The page title is "Enabling enterprise video surveillance with video analytics". The article is by Nik Gagvani, dated 06/19/2009. It discusses the migration of video surveillance from analog to modern digital systems and the use of video analytics for physical security and business intelligence. The sidebar features a "Refine your Google search" section with results related to Cisco subnet+blog, including articles about IPv6 security, Cisco and the UCS Channel, Cisco campaign aims to help channel partners through economic storm, and Cisco Knowledge Share.



IP Video Streaming Applications: Business Case

➤ IP Video Streaming Applications

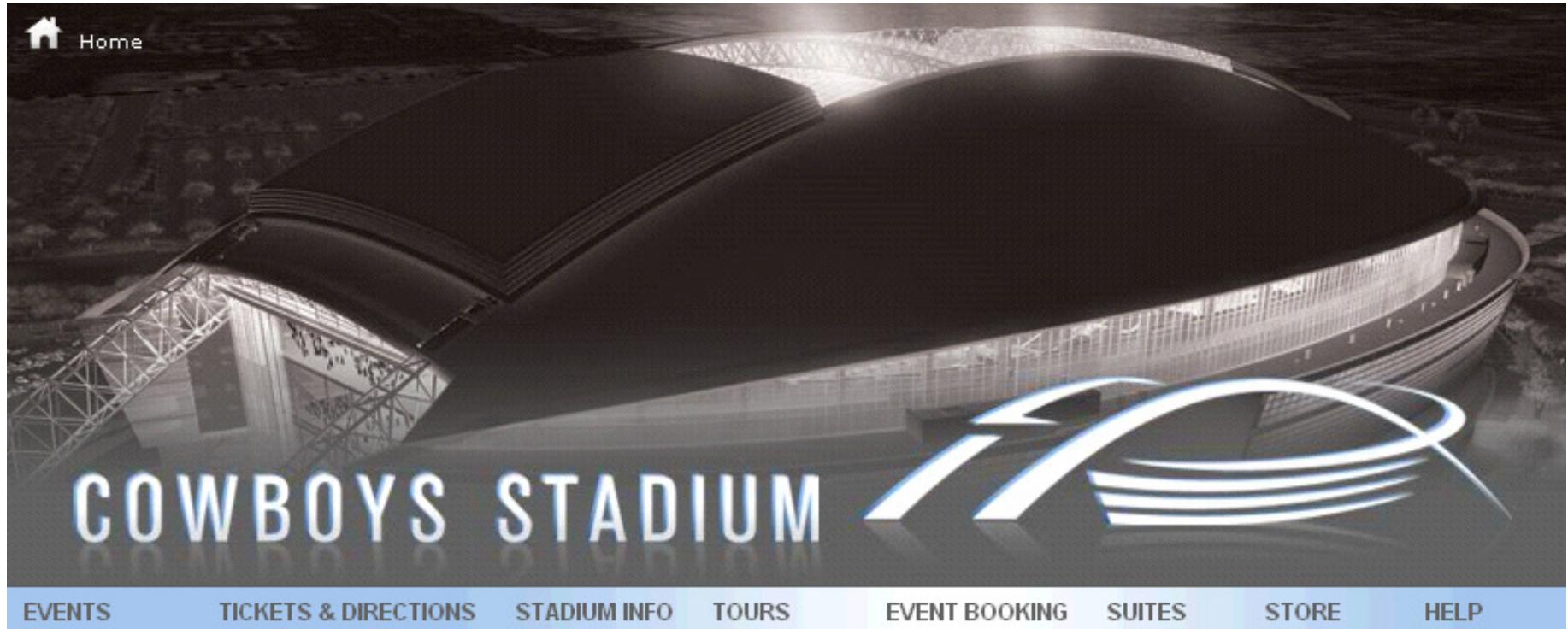
- Entertainment venues
- Professional sports stadiums

➤ Real-world examples

- “America’s Team”



Cowboys Stadium



The screenshot shows the Cowboys Stadium website. At the top left is a 'Home' button with a house icon. The main image is a night photograph of the stadium's illuminated retractable roof. Overlaid on the bottom left is the text 'COWBOYS STADIUM' in large, white, sans-serif letters. To its right is the Dallas Cowboys logo, which consists of a stylized 'D' formed by three concentric, swooping arcs. Below the main image is a navigation bar with the following links: EVENTS, TICKETS & DIRECTIONS, STADIUM INFO, TOURS, EVENT BOOKING (highlighted in blue), SUITES, STORE, and HELP.

Home

COWBOYS STADIUM

Dallas Cowboys logo

EVENTS TICKETS & DIRECTIONS STADIUM INFO TOURS EVENT BOOKING SUITES STORE HELP



Sipera Systems

Cowboys Stadium

Dallas Cowboys and Cisco ... http://newsroom.cisco.com/dlls/2009/prod_061709.html?sid=BAC-3sSynd

Solutions Products & Services Ordering Support Training & Events Partner Central

Worldwide [change] Log In | Register | About Cisco

Search Go

News@Cisco >
Press Release

Share, Email, SMS Print Subscribe

Dallas Cowboys and Cisco Kick Off Ultimate Fan Experience in Versatile New Stadium

Cowboys to Deploy Cisco Connected Sports Solutions in State-of-the-Art Venue

DALLAS, June 17, 2009 – Cisco today announced that the new Dallas Cowboys stadium has been outfitted with Cisco® Connected Sports technologies, making the largest National Football League stadium ever built also the most versatile and technologically advanced entertainment venue in all of North American football.

The newly opened 3 million-square-foot stadium, designed by HKS Sports and Entertainment Group, can host up to 100,000 fans for major sports or entertainment events. The stadium is designed to build on the international Cowboys brand while still maintaining the heritage of America's Team that Cowboys fans know and love.

The Cisco Connected Sports solution, deployed through a project with AT&T, will be central to the fan experience, will help the Cowboys create new revenue streams and provide the flexibility to adapt the stadium to support any number of events. Cisco StadiumVision™ integrates high-definition video, digital content and interactive fan services into one seamless next-generation network that transcends sports operations and connects the Cowboys, and the stadium, to its fans in entirely new ways. In addition to new sports and entertainment experiences, the Cowboys will use Cisco StadiumVision to maximize the value of their new home.

Enhanced Fan Experiences

- Fans remain engaged anywhere in the stadium, whether in the concourse, club or concessions areas, with nearly real-time, relevant information.

http://newsroom.cisco.com/dlls/features_filter.html?sort=date&filter=&dates=1,12

Photo

Cisco CEO John Chambers and Dallas Cowboys owner Jerry Jones shake hands at a press conference at the new Dallas Cowboys Stadium to announce the Cisco technology deployment.

News@Cisco

- Cisco News
- Events
- Press Releases
- Feature Stories
- Corporate Information
- Press Resources

World Wide News Sites

Select a country

Media

- Podcasts
- Videos
- Blogs
- SMS
- Flickr
- Facebook
- Twitter
- RSS Feeds
- My News@Cisco Wire

Pop-ups Blocked: 1



Sipera Systems

Cowboys Stadium

Dallas Cowboys deck out new stadium with Cisco video technology

By Jim Duffy, Network World, 06/17/2009

Share/Email Tweet This 1 Comment Print Newsletter Sign-Up

The Dallas Cowboys this week signed a deal to outfit their brand new stadium with immersive and interactive video technology from [Cisco](#).

The Cowboys will equip their \$1.1 billion stadium with Cisco Connected Sports technologies – including [Cisco StadiumVision](#) and IP phones and infrastructure. The technology provides sporting and events facilities with thousands of high-definition video monitors and digital signage customized for a particular event. StadiumVision also allows fans to interact with the event experience by taping and accessing instant replays on a handheld device and sharing it with other participants, or with anyone on the Internet.

Cisco StadiumVision is also in use at the new [Yankee Stadium](#) and at Toronto's [Rogers Centre](#), home of Major League Baseball's Toronto Blue Jays.

The deal between Cisco and the Cowboys makes the new 3 million square-foot Cowboys' Stadium the most technologically advanced entertainment venue in all of North American football. Cisco says. It even has the world's

White Paper
The Compelling Case for Video Telephony in UC: Download now

Refine your Google search

Your search on "cisco subnet+blog" also yielded these NetworkWorld results.

- IPv6 security guru fields questions**
Scott Hogg, the coauthor of the Cisco-approved IPv6 Security guidebook, talks discusses how networks...
May 6, 2009
- Cisco and the UCS Channel**
Cisco and the UCS Channel
March 23, 2009
- Cisco campaign aims to help channel partners through economic storm**
Cisco campaign aims to help channel partners through economic storm
February 20, 2009
- Check out Cisco Knowledge Share**
In today's newsletter I'd like to tell you about a fantastic resource at NetworkWorld.com, a relatively new blog on...
January 22, 2009

[View all search results](#)



Sipera Systems

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



Sipera Systems

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**



Sipera Systems

Yankee Stadium

The screenshot shows a Microsoft Internet Explorer window displaying a news article from NetworkWorld.com. The URL in the address bar is <http://www.networkworld.com/news/2008/111208-cisco-plans-networked-screens-at.html>. The page content discusses Cisco's plans to install networked screens at the new Yankee Stadium, featuring live game play and traffic information. The NetworkWorld navigation bar includes links for Security, LANs & WANs, VoIP, Infrastructure Mgmt, Wireless, Software, Data Center, SMB, Careers, Toolshed, and Communities. A sidebar on the right contains a Google search box and a list of related Cisco news articles.

Cisco plans networked screens at Yankee Stadium

By [Stephen Lawson](#), IDG News Service, 11/12/2008

The new Yankee Stadium in New York will have networked high-definition screens from [Cisco](#) that can show live game play and later switch to giving exit directions and traffic information.

The screens will be the first installation of [a product Cisco announced on Tuesday](#) in Manhattan, called Cisco StadiumVision. They also are the most visible element of a larger plan to use networking to enhance the audience experience at the stadium, which will open in April 2009. Cisco Chairman and CEO John Chambers and Yankees Co-Chairperson Hal Steinbrenner unveiled the plans at a press conference at Cisco's New York offices.

StadiumVision, designed specifically for stadiums and other venues, takes advantage of a technology called digital signage. The concept takes advantage of flat-screen displays and wired or wireless networks to provide signs that can change depending on time, situation and specific location.

At Yankee Stadium, they will show live games in progress throughout the stadium, including in

White Paper
Think You Have An Application Delivery Strategy? Download now

Refine your Google search

Your search on "cisco subnet+blog" also yielded these NetworkWorld results.

- IPv6 security guru fields questions
Scott Hogg, the coauthor of the Cisco-approved IPv6 Security guidebook, talks discusses how networks...
May 6, 2009
- Cisco and the UCS Channel
Cisco and the UCS Channel
March 23, 2009
- Cisco campaign aims to help channel partners through economic storm
Cisco campaign aims to help channel partners through economic storm
February 20, 2009
- Check out Cisco Knowledge Share
In today's newsletter I'd like to tell you about a fantastic resource at NetworkWorld.com, a relatively new blog on...
January 22, 2009

[View all search results](#)



Sipera Systems

Toronto Blue Jays

The screenshot shows a web browser window with the URL <http://www.networkworld.com/community/node/42168>. The page is titled "Blue Jays sign up for Cisco ...". The main content is an article from the Cisco Subnet Blog, dated Tue, 05/26/09 - 9:27pm, about the Toronto Blue Jays using Cisco StadiumVision. The article includes social sharing links (Share, Tweet This, Email this page, Comment, Print) and a "Newsletter Sign-Up" button. To the right of the article is an advertisement for Juniper Networks featuring a video player and text: "Learn how to drive down TCO and increase performance. Watch our Distributed Enterprise Solutions video →". Above the article, there's a banner for Juniper Networks and another for Microsoft Virtualization.



Sipera Systems

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.



Sipera Systems

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).



Sipera Systems

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.



Sipera Systems

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**



Sipera Systems

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



Sipera Systems

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)
```

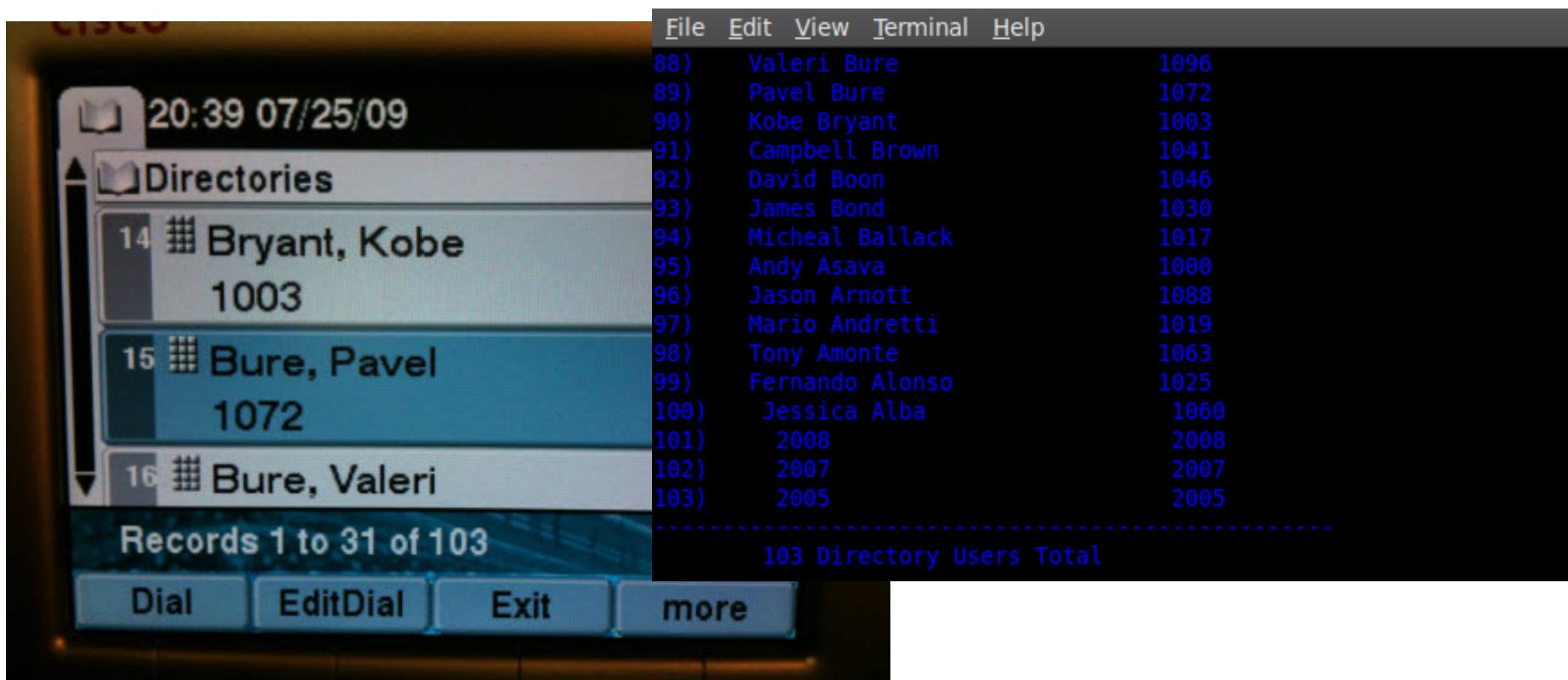
- **In security testing, time is money; therefore, you have to move fast. UCSniff wraps all necessary features into a single tool.**



Sipera Systems

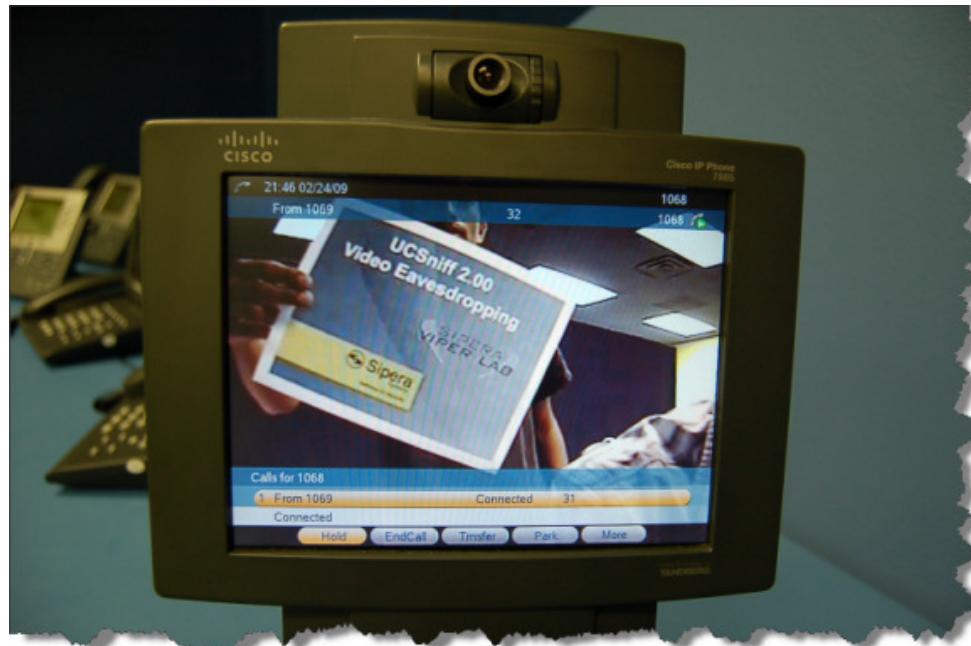
UCSniff 1.0

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



UCSniff 2.0

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



Sipera Systems

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



Sipera Systems

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.



Sipera Systems

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**



Sipera Systems

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.



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.**



Sipera Systems

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.



Sipera Systems

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



Sipera Systems

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



Sipera Systems

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.**



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**



Sipera Systems

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.

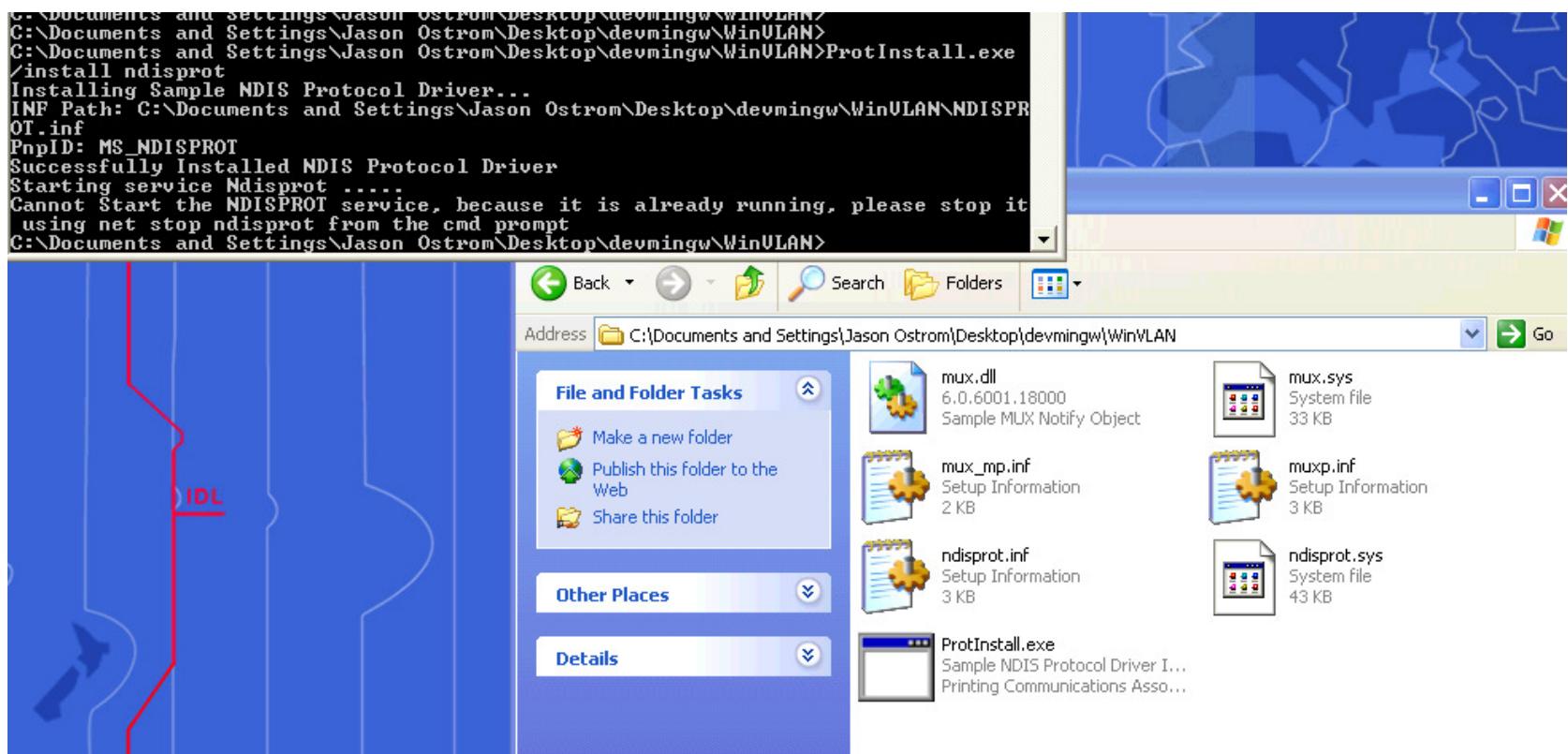


Sipera Systems

Installing Ndisprot

▪ Using ProtInstall - NDISPROT Driver Installer

- <http://www.ndis.com/papers/ndisinstall/programinstall.htm>



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>net start ndisprot
```

The Sample NDIS Protocol Driver service was started successfully.

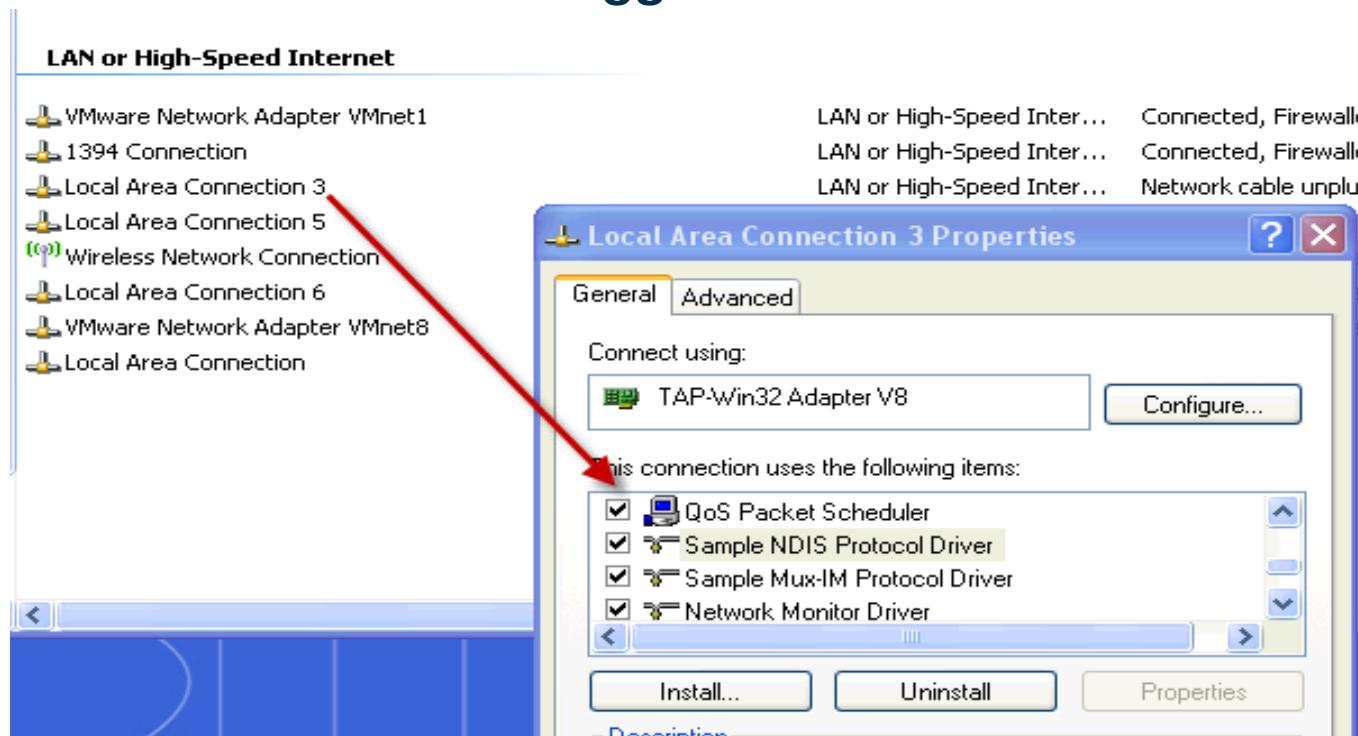
```
C:\Documents and Settings\Jason Ostrom>
```



Sipera Systems

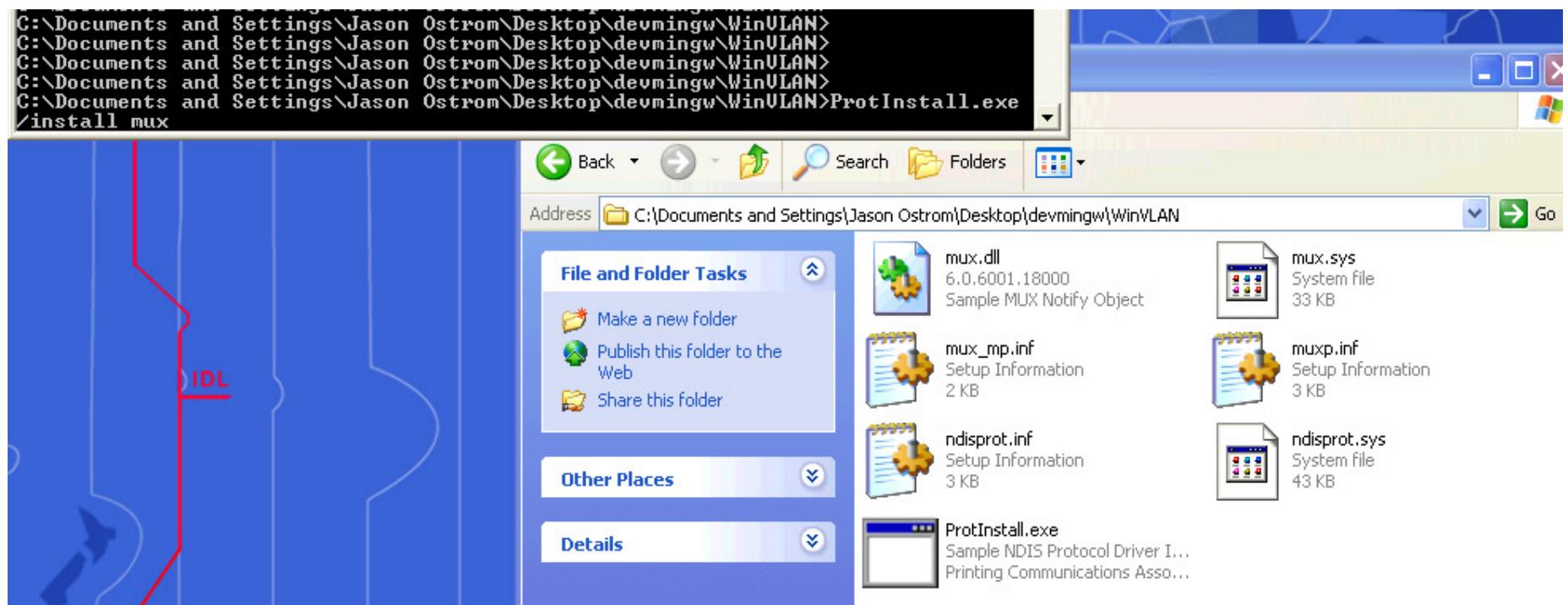
IM (Intermediate) Driver

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



Installing IM driver

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



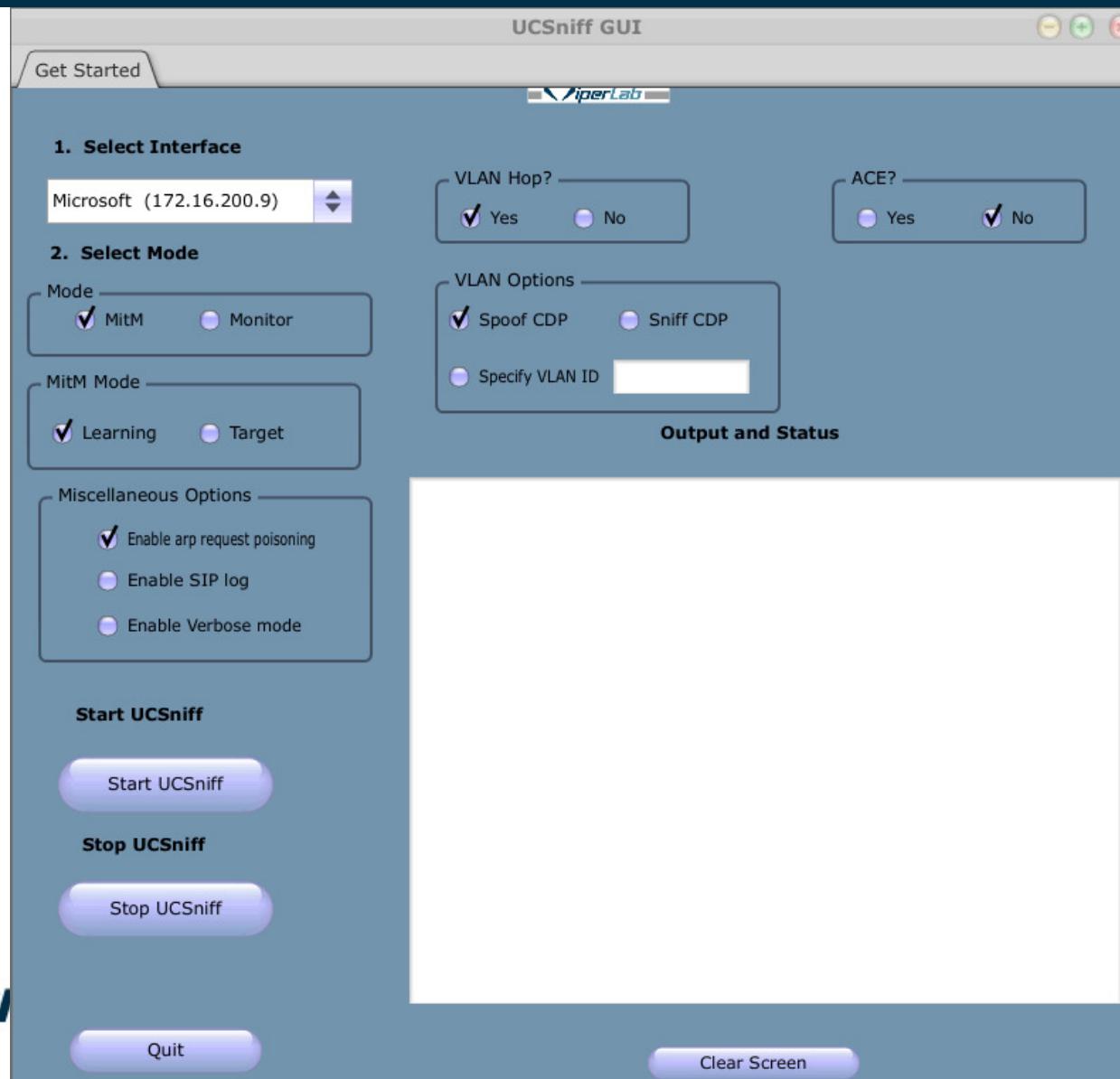
Video Decoding Support

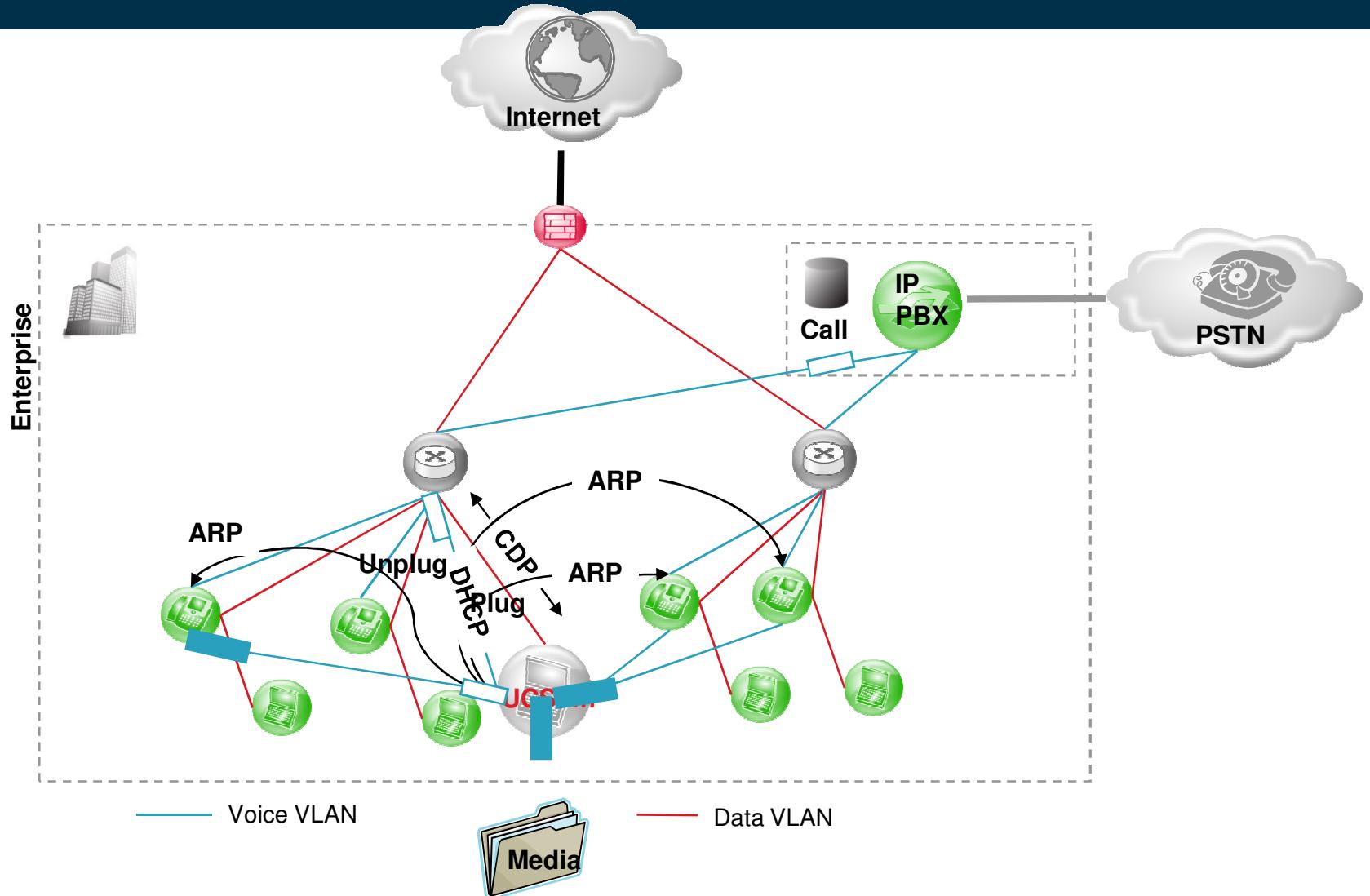
- Decodes H.264 content from RTP
- Compliant with RFC 3984 (RTP payload format for H.264 video codec)
- Creates a raw H.264 video only file, playable on VLC and Mplayer
- FFmpeg libraries
 - AVI Container
 - Muxing audio and video



Sipera Systems

UCSniff Overview





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

A screenshot of an MPlayer window displaying a video feed. The video shows a person from the chest up, wearing a light-colored t-shirt and a dark lanyard with a badge. The background is slightly blurred, suggesting an indoor office environment.

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**



Sipera Systems

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

```
[+] Active Video call from Extension 1068 (172.16.99.4) --> Extension 1069 (172.16.99.5)
[+] Press 'a' from help menu to begin attack against active Call Session.

Index      Call Session
-----
[1]        Ext: 1068(172.16.99.4) --> Ext: 1069(172.16.99.5)
-----

[+] Only 1 call with index [1] detected
[+] Enter the active session index to attack: [1]

[+] Options for VideoJak attack:
[1] Run attack against Extension 1068, IP Video Phone target 172.16.99.4
[2] Run attack against 1069, IP Video Phone target 172.16.99.5

[+] Enter the option indicating IP Phone to run attack against:

[+] Option 1 selected. Attacking Active SCCP Call Session against Extension 1068, IP Video Phone target 172.16.99.4
[+] Please wait while VideoJak gathers required Attack data.
[+] Searching for Audio and Video RTP Streams in the pcap handle.
[+] Successfully Gathered needed Attack data.
[+] Starting attack against the target IP Video Phone. Use Ctrl-C to stop the attack.
```



Sipera Systems

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



Sipera Systems

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



Sipera Systems

VideoJak Development

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

No.	Time	Source	Destination	Protocol	Info
121	1.069552	172.16.100.3	172.16.100.2	TCP	timbuktu-srv1 > rtsp [SYN] Seq=1 Win=65352 Len=0 MSS=1460
122	1.069555	172.16.100.3	172.16.100.2	TCP	rtsp > timbuktu-srv1 [SYN, ACK] seq=0 Ack=1 win=5840 Len=0 MSS=1460
123	1.069641	172.16.100.3	172.16.100.2	TCP	timbuktu-srv1 > rtsp [ACK] Seq=1 Ack=1 win=6535 Len=0
124	1.069965	172.16.100.2	172.16.100.3	RTSP	OPTIONS rtsp://172.16.100.3:554/streamingSetting?version=1.0&sessionId=311346
125	1.070197	172.16.100.3	172.16.100.2	TCP	rtsp > timbuktu-srv1 [ACK] Seq=1 Ack=233 win=6432 Len=0
126	1.072414	172.16.100.3	172.16.100.2	RTSP	Reply: RTSP/1.0 200 OK
127	1.073630	172.16.100.2	172.16.100.3	RTSP	DESCRIBE rtsp://172.16.100.3:554/streamingSetting?version=1.0&sessionId=31134
128	1.076001	172.16.100.3	172.16.100.2	RTSP/SDP	Reply: RTSP/1.0 200 OK, with session description[Malformed Packet]
129	1.081757	172.16.100.2	228.67.43.91	UDP	Source port: 15947 Destination port: 15947
130	1.085549	172.16.100.2	172.16.100.3	RTSP	SETUP rtsp://172.16.100.3/ChannelID=1&ChannelName=Channel1/track2 RTSP/1.0
131	1.087369	172.16.100.3	172.16.100.2	RTSP	Reply: RTSP/1.0 200 OK
132	1.088617	172.16.100.2	172.16.100.3	RTSP	SETUP rtsp://172.16.100.3/ChannelID=1&ChannelName=Channel1/track1 RTSP/1.0
133	1.090054	172.16.100.3	172.16.100.2	RTSP	Reply: RTSP/1.0 200 OK
134	1.106771	172.16.100.2	172.16.100.3	RTSP	PLAY rtsp://172.16.100.3/ChannelID=1&ChannelName=Channel1/ RTSP/1.0
135	1.107941	172.16.100.3	172.16.100.2	RTSP	Reply: RTSP/1.0 200 OK
136	1.113954	172.16.100.3	172.16.100.2	H264	PT=Unknown (96), SSRC=0x73D5BF49, seq=13577, Time=10386000 FU-A
137	1.113978	172.16.100.3	172.16.100.2	H264	PT=Unknown (96), SSRC=0x73D5BF49, seq=13578, Time=10386000 FU-A
138	1.114095	172.16.100.3	172.16.100.2	H264	PT=Unknown (96), SSRC=0x73D5BF49, seq=13579, Time=10386000 FU-A
139	1.114262	172.16.100.3	172.16.100.2	H264	PT=Unknown (96), SSRC=0x73D5BF49, seq=13580, Time=10386000 FU-A
140	1.114262	172.16.100.3	172.16.100.2	H264	PT=Unknown (96), SSRC=0x73D5BF49, seq=13581, Time=10386000 FU-A

Frame 128 (727 bytes on wire, 727 bytes captured)
Ethernet II, Src: Cisco_Fd:df:9e (00:21:1b:fd:df:9e), Dst: 06:0a:25:78:2d:28 (06:0a:25:78:2d:28)
Internet Protocol, Src: 172.16.100.3 (172.16.100.3), Dst: 172.16.100.2 (172.16.100.2)
Transmission Control Protocol, Src Port: rtsp (554), Dst Port: timbuktu-srv1 (1417), Seq: 123, Ack: 491, Len: 673
Real Time Streaming Protocol
Response: RTSP/1.0 200 OK\r\nCSeq: 2\r\nDate: Tue, Jan 01 2008 00:03:15 GMT\r\nContent-Base: rtsp://172.16.100.3/ChannelID=1&ChannelName=Channel1/\r\nContent-type: application/sdp\r\nContent-length: 487\r\n\r\nSession Description Protocol
[Malformed Packet: SDP]



Sipera Systems

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:
 - Original RTP stream's SSRC
 - Payload Type
 - Incremented sequence and timestamp values
 - Spoofed source IP and UDP port of valid video sender



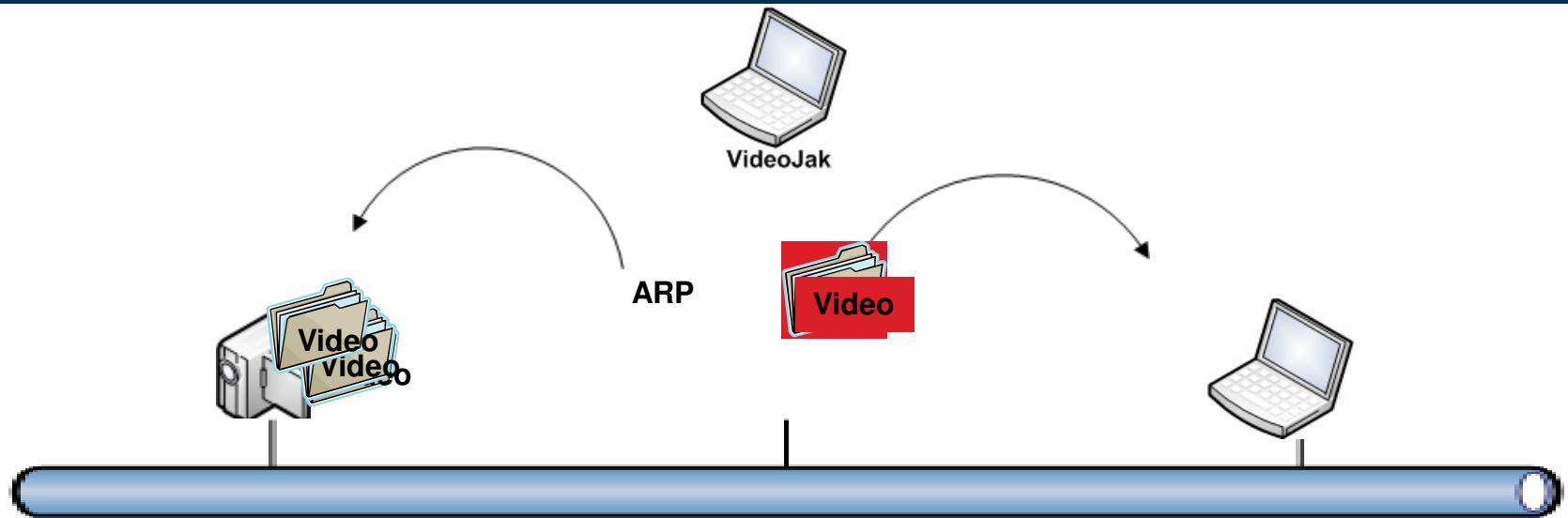
Sipera Systems

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

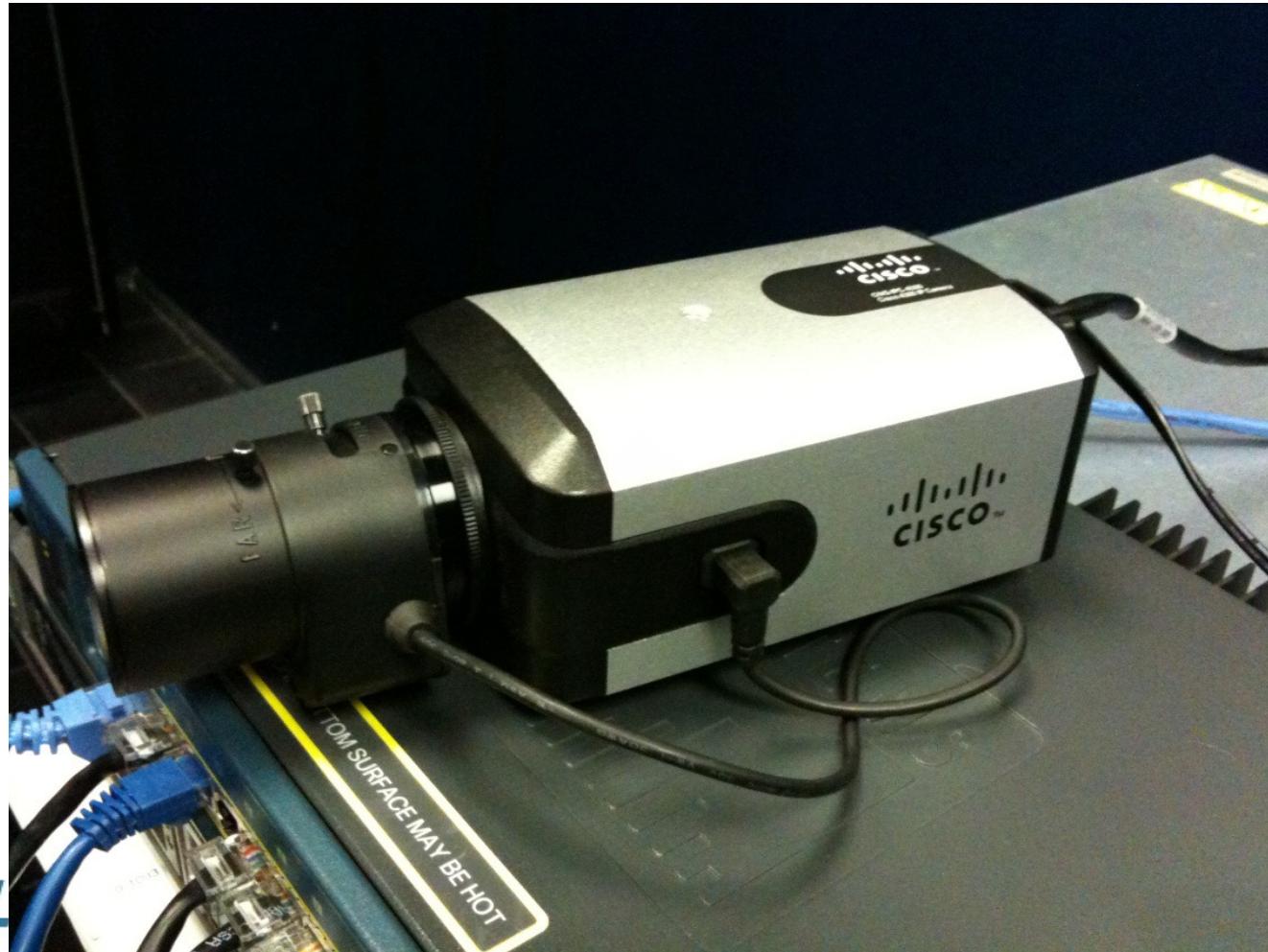


Sipera Systems



VideoJak Target

Cisco 4300 Series IP Camera



Sipera Systems

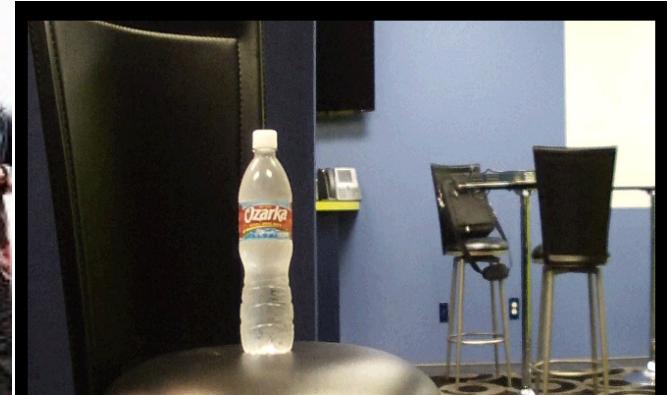
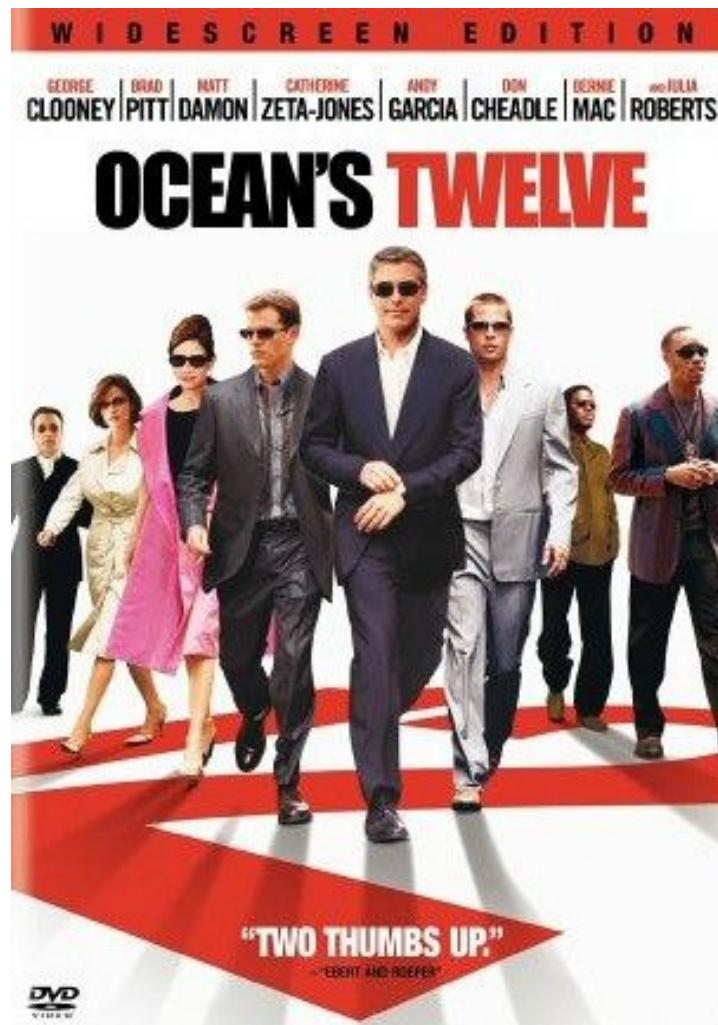
VideoJak Targets

- **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.**



Sipera Systems

VideoJak Tool Demo



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**



Sipera Systems

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.**

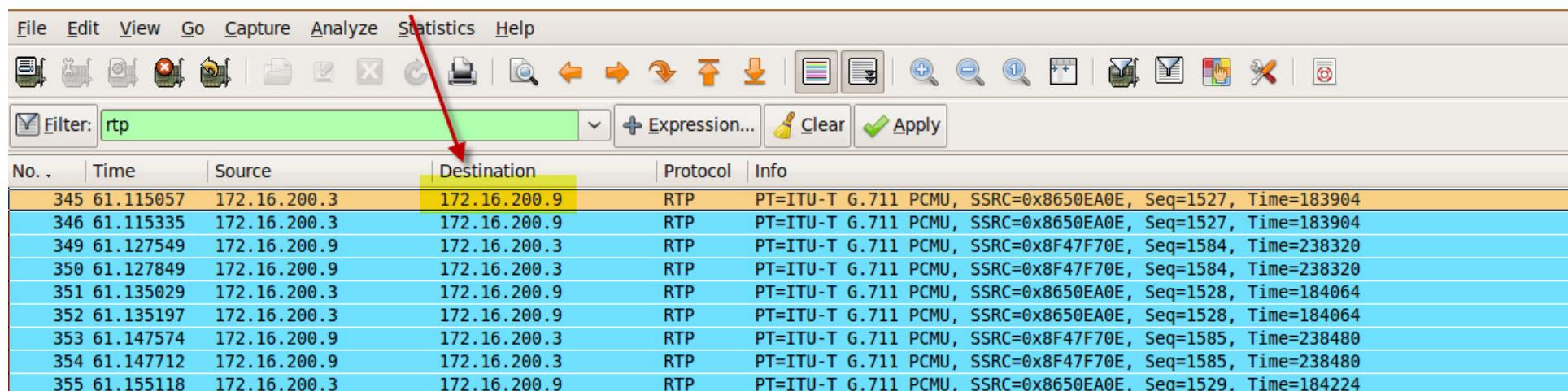


Sipera Systems

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



The screenshot shows the Wireshark interface with a green filter bar containing 'rtp'. The main window displays a list of RTP packets. A red arrow points to the 'Destination' column header. The table has the following structure:

No.	Time	Source	Destination	Protocol	Info
345	61.115057	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1527, Time=183904
346	61.115335	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1527, Time=183904
349	61.127549	172.16.200.9	172.16.200.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8F47F70E, Seq=1584, Time=238320
350	61.127849	172.16.200.9	172.16.200.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8F47F70E, Seq=1584, Time=238320
351	61.135029	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1528, Time=184064
352	61.135197	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1528, Time=184064
353	61.147574	172.16.200.9	172.16.200.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8F47F70E, Seq=1585, Time=238480
354	61.147712	172.16.200.9	172.16.200.3	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8F47F70E, Seq=1585, Time=238480
355	61.155118	172.16.200.3	172.16.200.9	RTP	PT=ITU-T G.711 PCMU, SSRC=0x8650EA0E, Seq=1529, Time=184224

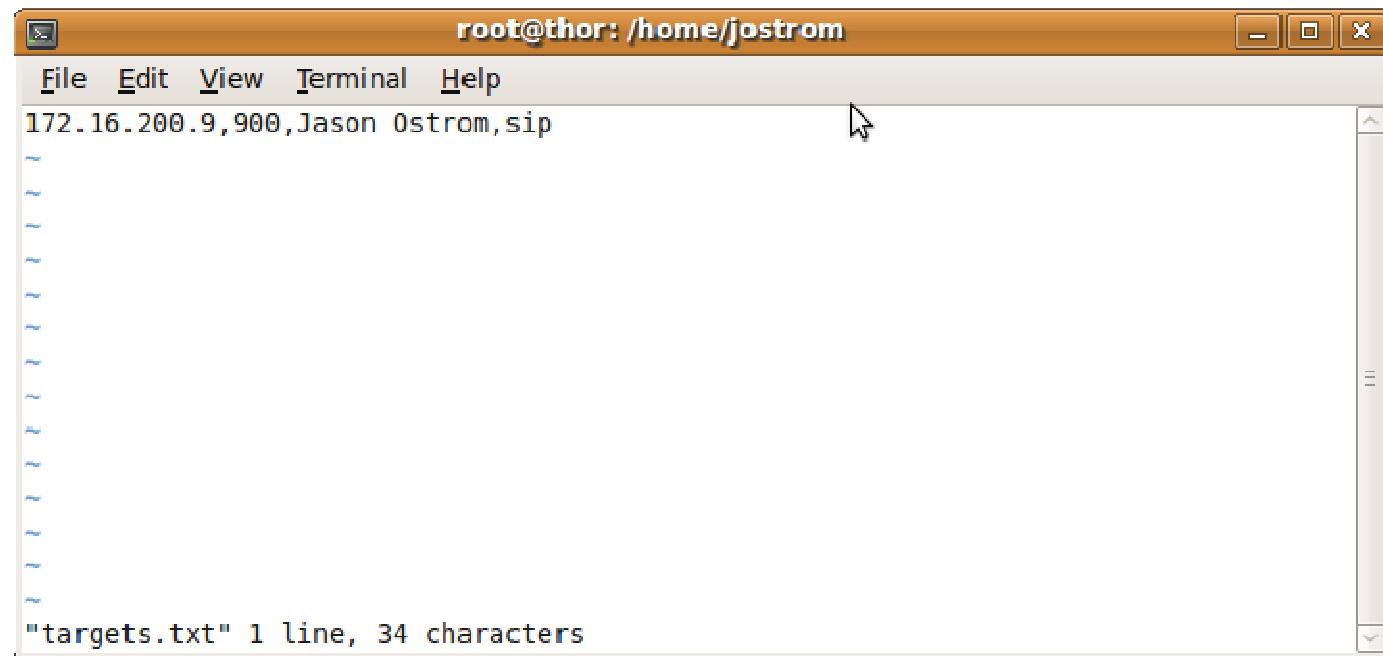


Sipera Systems

Create Targets Entry

- **Manually create file targets.txt**

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



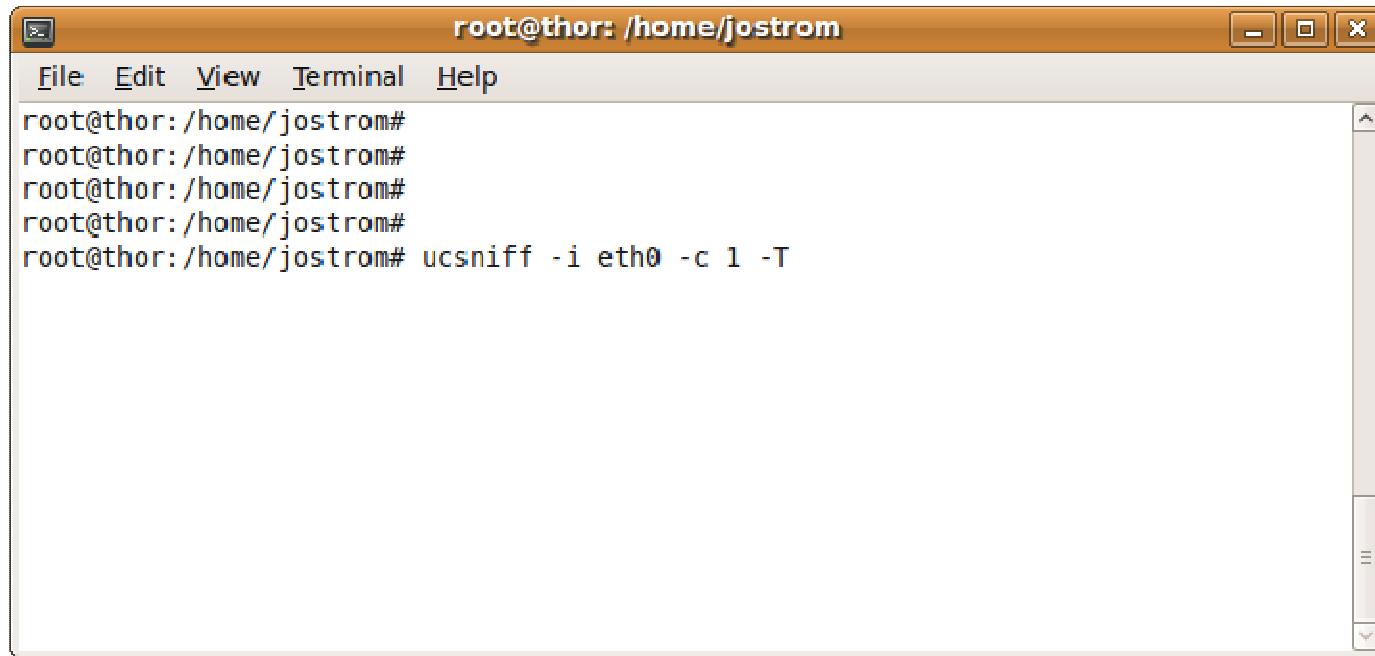
A screenshot of a terminal window titled "root@thor: /home/jostrom". The window contains the following text:

```
File Edit View Terminal Help
172.16.200.9,900,Jason Ostrom,sip
"targets.txt" 1 line, 34 characters
```

The terminal window has a standard window title bar with minimize, maximize, and close buttons. The menu bar includes File, Edit, View, Terminal, and Help. The main pane shows the command entered and its output. The status bar at the bottom indicates the file name and its size.

UCSniff Target Mode

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



A screenshot of a terminal window titled "root@thor: /home/jostrom". The window has a standard Linux-style title bar with icons for minimize, maximize, and close. The menu bar includes "File", "Edit", "View", "Terminal", and "Help". The terminal itself shows several blank lines of text, followed by the command "root@thor: /home/jostrom# ucsniff -i eth0 -c 1 -T". The terminal is set against a light gray background with a vertical scroll bar on the right side.

Select Targeted User

- Select targeted user

The screenshot shows a terminal window titled "root@thor: /home/jostrom". The window contains the following text:

```
Single user mode selected

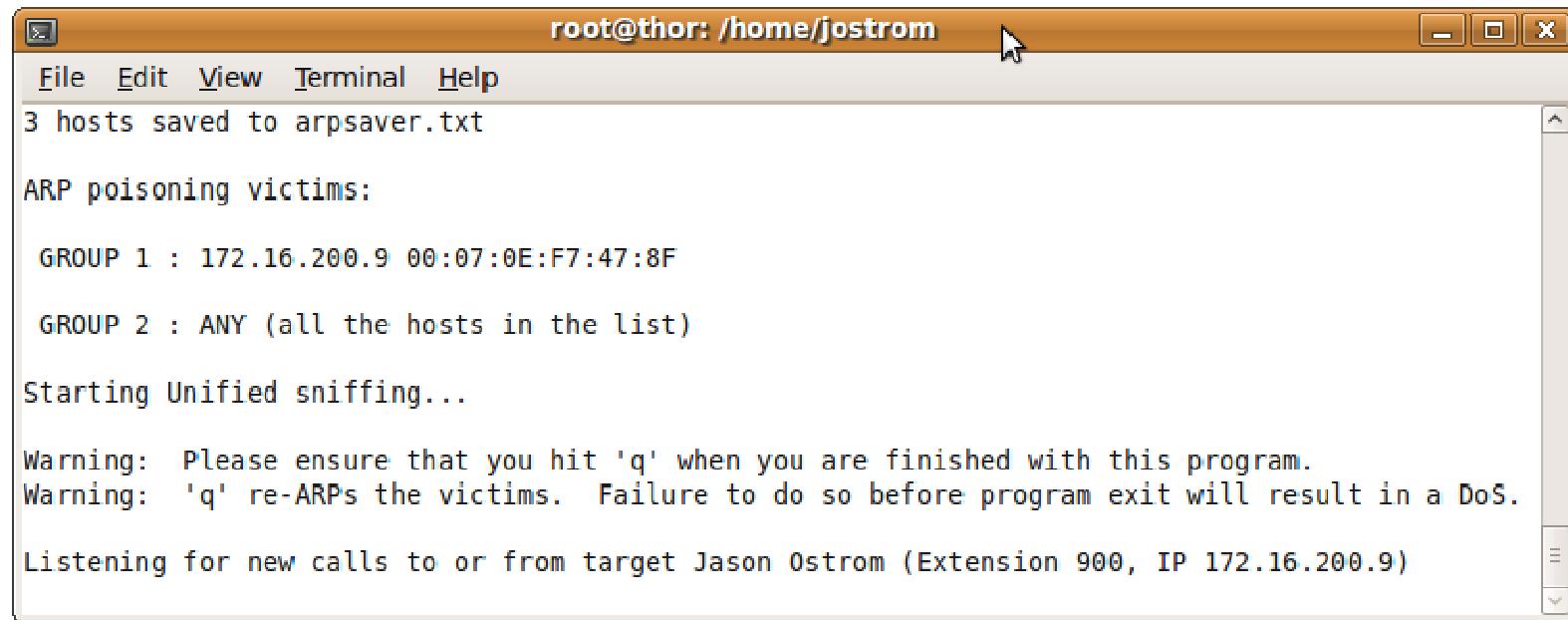
In this mode, you select one IP Phone Endpoint (User / Extension), and all calls to
or from this endpoint are targeted for eavesdropping

Displaying the discovered targets list:
-----
Extension      Name          IP        Protocol
-----
1)  900        Jason Ostrom  172.16.200.9  sip
-----

Please select one endpoint (1 - 1) from the discovered targets list:
1
```

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



The screenshot shows a terminal window titled "root@thor: /home/jostrom". The window contains the following text output from the UCSniff command:

```
root@thor: /home/jostrom
File Edit View Terminal Help
3 hosts saved to arpsaver.txt
ARP poisoning victims:
GROUP 1 : 172.16.200.9 00:07:0E:F7:47:8F
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 program.
Warning: 'q' re-ARPs the victims. Failure to do so before program exit will result in a DoS.
Listening for new calls to or from target Jason Ostrom (Extension 900, IP 172.16.200.9)
```

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)**



Sipera Systems

Background of a Live UC Pentest

- The “GARP Disabled” feature was getting in the way of a very successful pentest



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?**



Sipera Systems

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

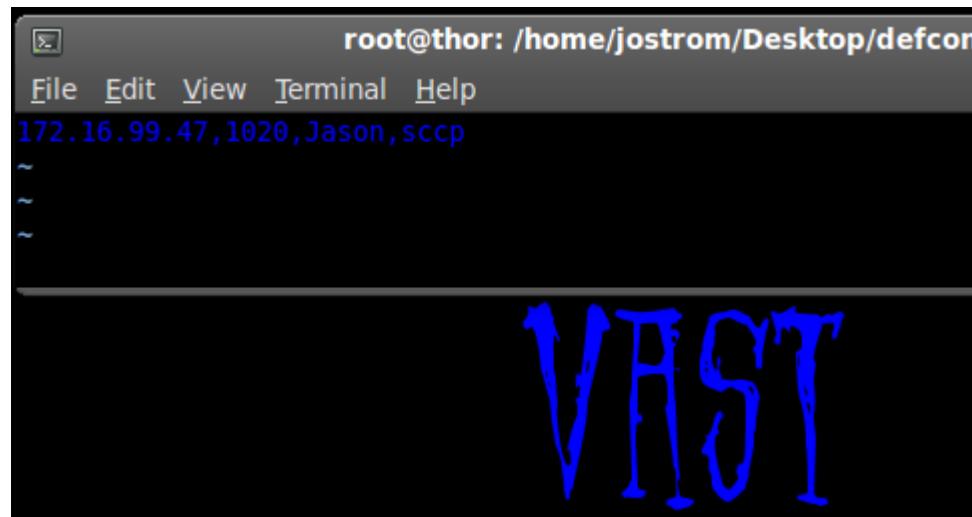


Sipera Systems

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



A terminal window titled "root@thor: /home/jostrom/Desktop/defcon". The window shows the command "172.16.99.47,1020,Jason,sccp" being typed into the terminal. The text "VRST" is displayed in large blue letters across the bottom of the terminal window.

```
root@thor: /home/jostrom/Desktop/defcon
File Edit View Terminal Help
172.16.99.47,1020,Jason,sccp
~
~
~
VRST
```

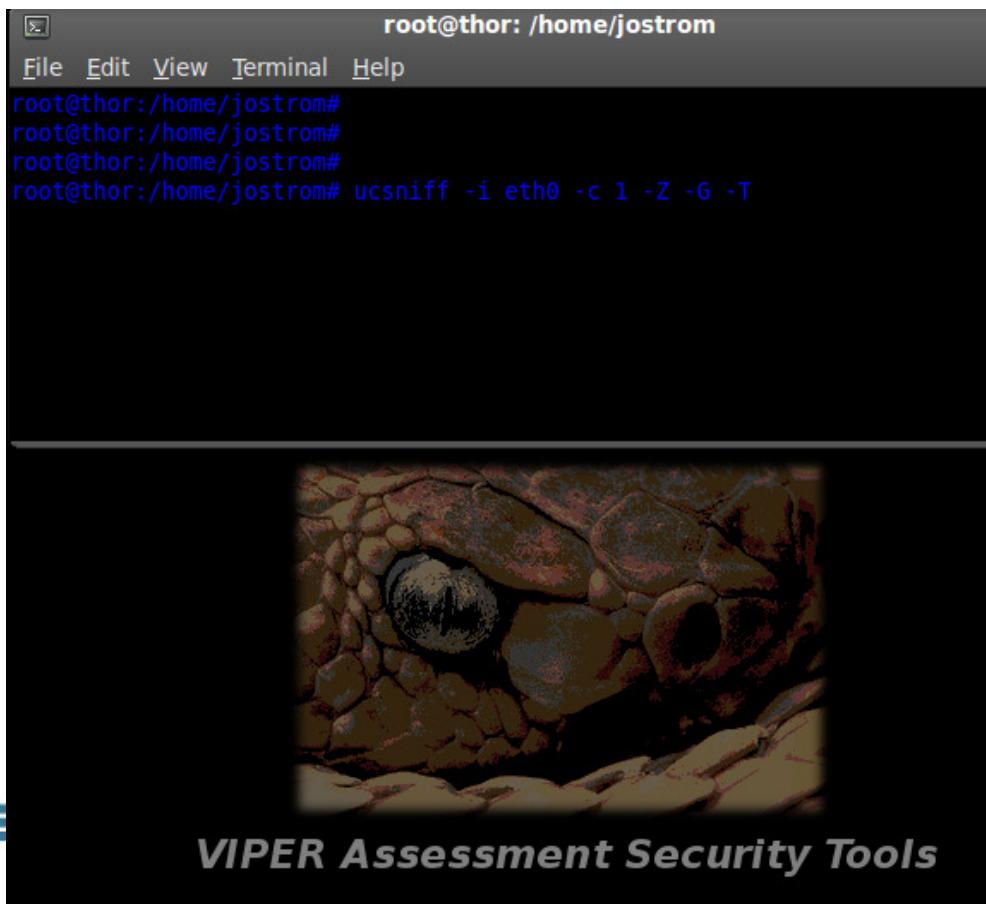


Sipera Systems

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



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
```



Sipera Systems

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



Sipera Systems

Step 3: Modify configuration setting for GARP via UDP Stream

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

```
<speaker><datse</disab  
et><forwardingDelay>1</  
ess><garp>1</garp><voic  
ty><autoSlectLineEnabl  
ctive>1 7</daysDispla
```

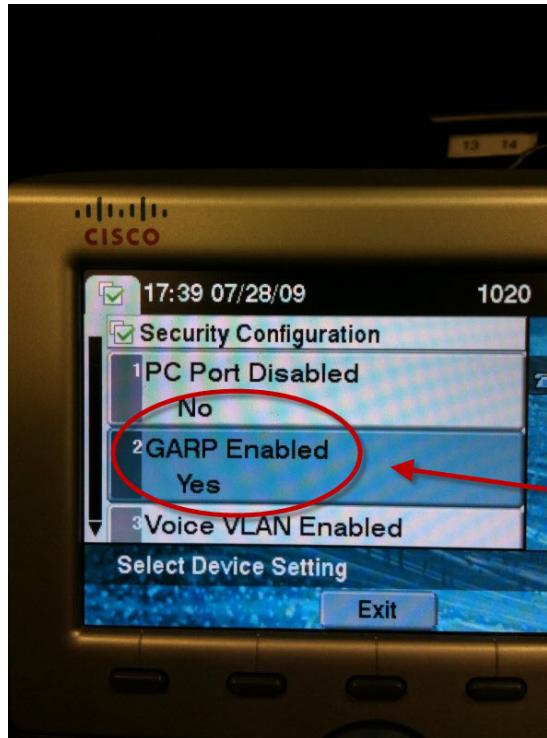
- To “GARP Enabled”

```
<speaker><datse</disab  
><forwardingDelay>1<,  
s><garp>0</garp><voic  
><autoSlectLineEnabl  
ctive>1 7</daysDispla
```

```
Dropping KeepAliveAckMessage: 172.16.100.1 --> 172.16.99.47  
Receiving SEP CNF XML file via TFTP MitM attack  
Modified the GARP Setting to GARP Enabled
```

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



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



Sipera Systems

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>



Sipera Systems

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>**



Sipera Systems