"Security behind the dial tone…"

VoIP Security Threats, Vulnerabilities, Countermeasures, and Best Practices

Peter Thermos
Principal Consultant
peter.thermos@palindrometech.com
Tel: 732 688 0413

ISSA Meeting 03/08

Speaker Background

- Consulting
  - Government and commercial organizations, consulting on information security and assurance, InfoSec program development and management, vulnerability assessments, security architecture, NGN/VoIP/IMS.
- Research
  - Principal investigator on research tasks, in the area of Internet Multimedia and Next Generation Networks (VoIP) and security, that were are funded by government organizations such as NIST (National Institute of Standards and Technology), DARPA (Defense Advanced Research Agency), NSF (National Science Foundation) and others. In addition he has been working with domestic and foreign Telecommunications carriers and Fortune 500 companies on identifying security requirements for IMS/NGN and VoIP, conducting vulnerability assessments and product evaluations.
- Member of IETF/IEEE/ACM.
- Education
  - MS,CS Columbia University

Outline

- Intro – Present and Future
- Components & Protocols
- Security – Threats, Attacks & Vulnerabilities
- Best Practices
- Assessment Tools
- Conclusions
- Additional Information for bedtime reading…

Present and Future (Summary)

PSTN Network

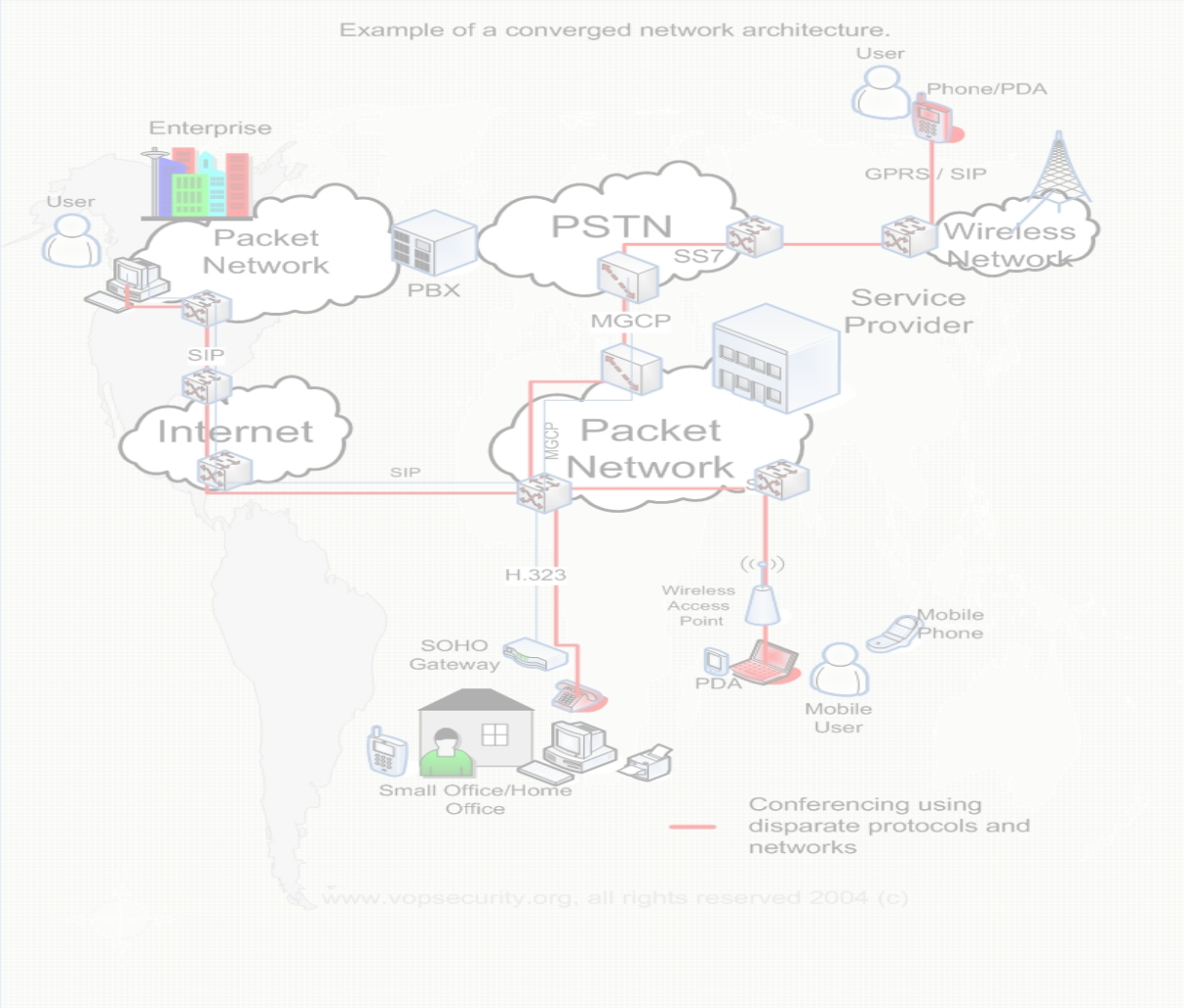
- Closed therefore “secure”
- High availability (99.999%)
- Limited connection to IP (OSS provisioning, management)

IP Network

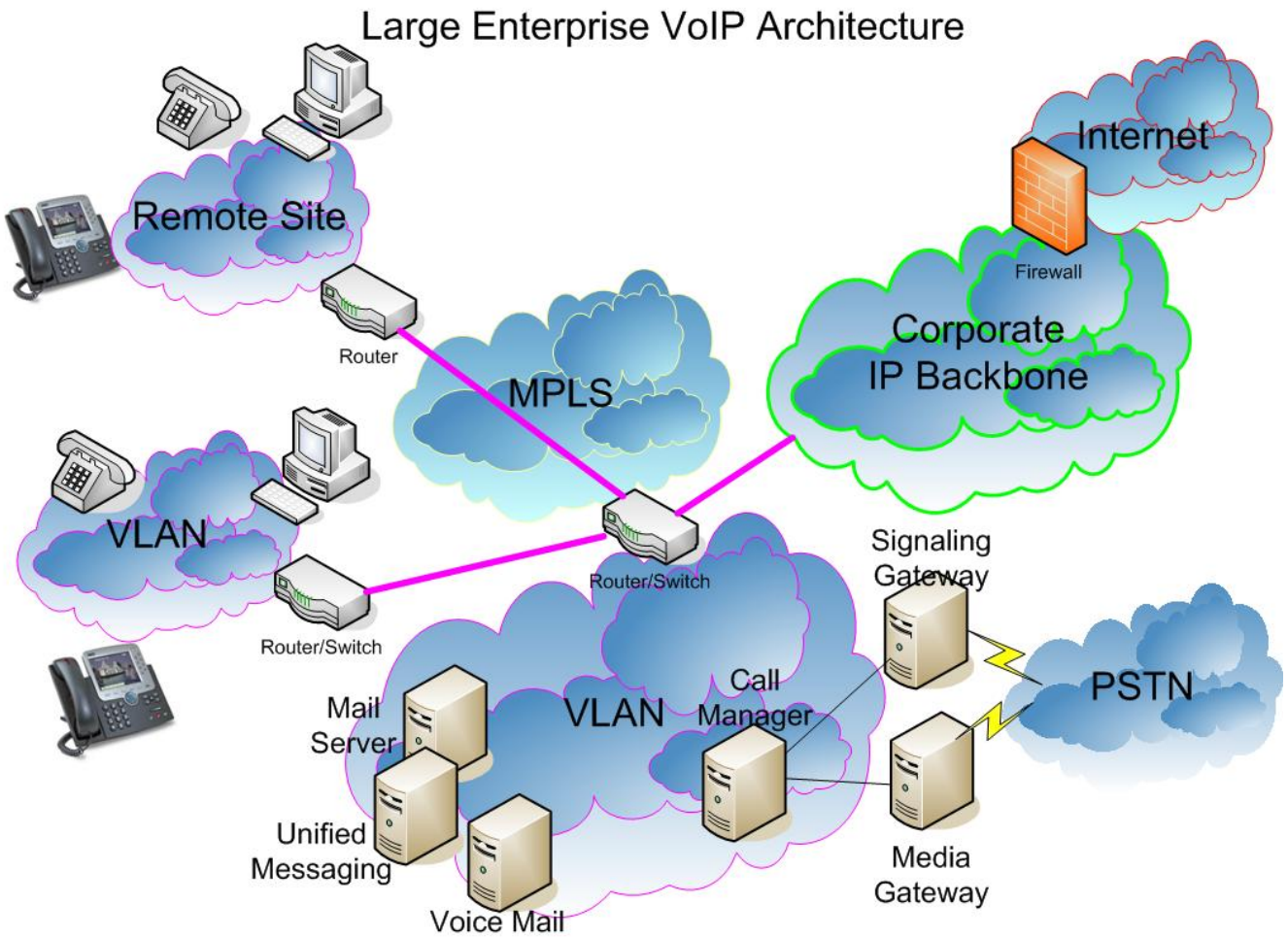
- Loose access controls.
- Best effort
- Connected to accessible IP networks.

“There is one safeguard known generally to the wise,
which is an advantage and security to all,
but especially to democracies as against despots.
What is it? Distrust. ”.
Demosthenes (c. 384–322 B.C.), Greek orator. Second Philippic, sct. 24 (344 B.C.)

The Future – The Converged Network



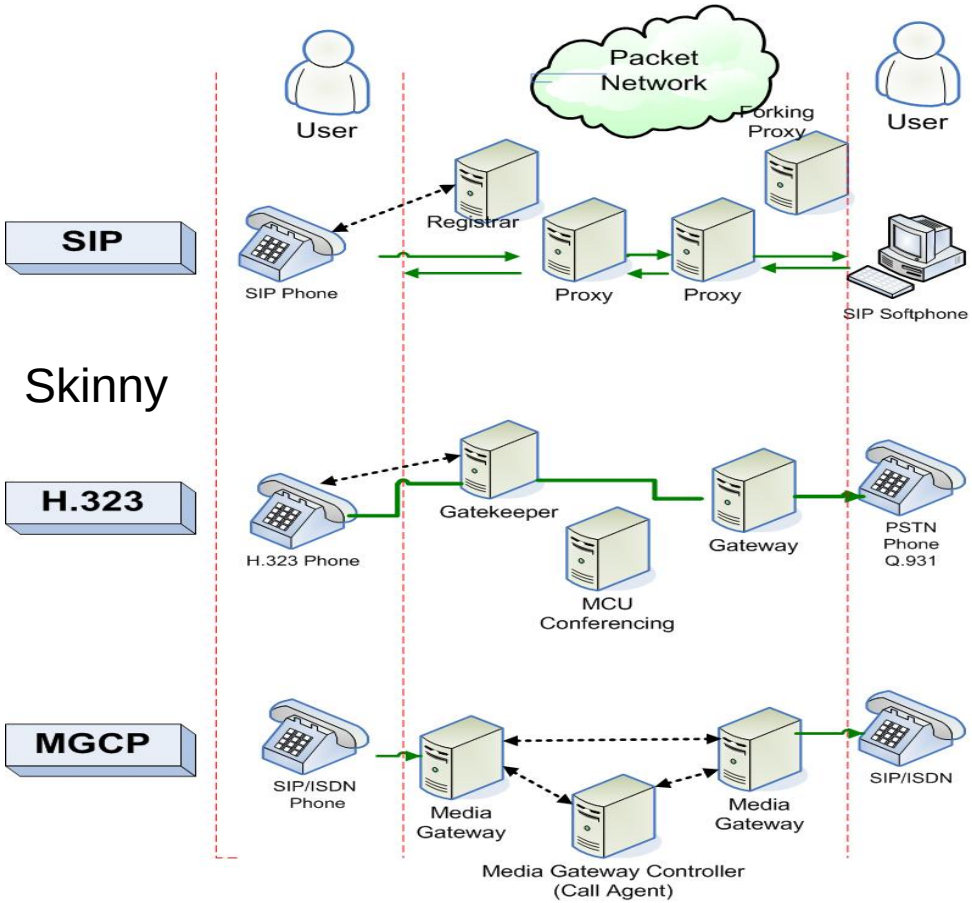
Enterprise VoIP Architecture (a case-study)



Lessons learned

- Evaluate your architecture design BEFORE you go forward for deployment.
- Security evaluation of architecture and testing of pilot infrastructure identified inconsistencies that helped improve design and configuration for production environment and future evolution of the network.

Components and Signaling Protocols



Outline

- Intro – Present and Future
- Components & Protocols
- **Security – Threats, Attacks & Vulnerabilities**
- Best Practices
- Assessment Tools
- Conclusions
- Additional Information for bedtime reading…

Threats and Attacks

Threats	Target(s)
Service disruption (amplification attacks DoS/DDoS)	Network Owners, Service Providers, Subscribers
Eavesdropping (including traffic analysis)	Network Owners, Service Providers, Subscribers
Fraud (including service and intellectual assets, confidential information)	Network Owners, Service Providers
Unauthorized access (compromise systems with intentions to attack other systems or exploit vulnerabilities to commit fraud and eavesdropping).	Network Owners, Service Providers, Subscribers
Annoyance (e.g. SPIT)	Subscribers

See also the VoIPSA taxonomy for a more detailed outline.

Attack Categories

- Service disruption (DoS/DDoS)
  - Against phones, proxies, routers
  - SIP/MGCP/H.323/RTP
  - Affects edge-devices, overloads signaling elements and consumes network bandwidth
- Unauthorized access
  - Network elements including subscriber devices, voice mail, email, DNS, NTP, DHCP servers.
  - Service (i.e., ssh, HTTP)
  - Applications (i.e., SQL injection, CSS-CSRF)
  - Management systems
  - Provisioning Systems
  - Billing Systems
- Eavesdropping and traffic analysis
- Fraud
  - Network element compromise
  - Manipulating the signaling messages and/or call flow

1st Case of VoIP Fraud

- FBI arrests two for VoIP Fraud Pena, Moore
  - http://www.foxnews.com/story/0,2933,198778,00.html
- Duration ~ 8-12 months
- Revenue/Fraud $1M
- Attack Objective: Compromise service VoIP service providers and enterprise networks that support VoIP to route unauthorized VoIP traffic originating from Telecom carriers.
- Upstream provider pays fraudster, downstream provider doesn't know.

Other Internet Phone related Fraud

- Phone fraud in Moldova-
  - In another interesting case that raises novel issues, a federal court in New York granted the Federal Trade Commission's request for a temporary restraining order to shut down an alleged scam on the World Wide Web. According to the FTC's complaint, people who visited pornographic Web sites were told they had to download a special computer program. Unknown to them, the program secretly rerouted their phone calls from their own local Internet provider to a phone number in Moldova, a former Soviet republic, for which a charge of more than two dollars a minute could be billed. According to the FTC, more than 800,000 minutes of calling time were billed to U.S. customers. http://www.cybercrime.gov/sentechtest.htm

Where are the vulnerabilities?

- Threat model, vulnerabilities originate from the difficulty to foresee future threats (e.g. Signaling System No.7)
- Design & specification vulnerabilities come from errors or oversights in the design of the protocol that make it inherently vulnerable (e.g., SIP, MCGP, 802.11b)
- Implementation vulnerabilities are vulnerabilities that are introduced by errors in a protocol implementation
- Architecture, network topology and association (e.g. routing) with other network elements.

Top 14 VoIP Vulnerabilities

- 1. **Insufficient verification of data**: In VoIP implementations, this can enable man-in the-middle attacks.
- 2. **Execution flaws**: Standard databases are typically used as the backbone of VoIP services and registrations. Implementation has to be paranoid in filtering out active content such as SQL queries from user-provided data such as user names, passwords, and Session Initiation Protocol (SIP) URLs. The majority of problems relating to execution flaws result from bad input filtering and insecure programming practices.
- 3. **String/array/pointer manipulation flaws**: Malformed packets with unexpected structures and content can exist in any protocol messages, including SIP, H.323, SDP, MGCP, RTP, and SRTP. Most typical malformed messages include buffer-overflow attacks and other boundary-value conditions. The result is that the input given by the attacker is written over other internal memory content, such as registers and pointers, which will let the attacker take full control of the vulnerable process.

Top 14 VoIP Vulnerabilities (con'ed)

- 4. **Low resources**: Especially in embedded devices, the resources that VoIP implementations can use can be scarce. Low memory and processing capability could make it easy for an attacker to shut down VoIP services in embedded devices.

- 5. **Low bandwidth**: The service has to be built so that it will withstand the load even if every caller makes a call at the same time. When the number of subscribers to a VoIP service is low, this is not a big problem. But when a service is intentionally flooded with thousands of bot clients, or when there is an incident that results in a huge load by valid subscribers, the result might be a shutdown of the whole service.

- 6. **File/resource manipulation flaws**: These are typical implementation mistakes, programming errors from using insecure programming constructs that result in security problems. These flaws include insecure access to files.

Top 14 VoIP Vulnerabilities (con'ed)

- 7. **Password management**: The only identifier a VoIP consumer has is the telephone number or SIP URL and a possible password for the service. The passwords are stored in both the client and server. If passwords are storied in the server in a format that can be reversed, anyone with access to that server (or proxy or registrar) can collect the username and password pairs.

- 8. **Permissions and privileges**: Resources have to be protected both from the operating system and platform perspective and from the network perspective. VoIP services running on the platform have to consider the privileges they run with. A VoIP service does not necessarily require administrative or "root" privilege to run.

- 9. **Crypto and randomness**: In VoIP signaling, confidential data needs to be protected from eavesdropping attacks. The most common vulnerability in this category is to fail to encrypt at all, even if the encryption mechanisms are available.

- 10. **Authentication and certificate errors**: Users and devices need to be authenticated. Also, other services, such as device management, exist in VoIP devices that need user authentication. Registration hijack in SIP is a flaw in which the registrar system does not authenticate the user or device, but lets attackers spoof registration messages and reregister themselves as the valid user.

Top 14 VoIP Vulnerabilities (con'ed)

- 11. **Error handling**: One example of error handling in SIP implementations is how incorrect registration is handled. A register message with an invalid telephone number can result in a "404" error code, whereas a valid telephone number would result in a "401" error. This will let the attacker narrow down the attack to try a brute-force attack on valid accounts only, or to harvest for valid accounts for Spam over Internet Telephony (SPIT).
- 12. **Homogeneous network**: An unpredicted vulnerability in many network infrastructures is a wide dependence on a limited number of vendor brands and devices variants. If an entire network depends on one specific brand of phone, proxy or firewall, one automated attack such as a virus or worm can shut down the entire network.
- 13. **Lacking fallback system**: When the VoIP network is down, as it eventually will be, there has to be backup systems that the users can fall back to. This requires careful planning for the infrastructure.
- 14. **Physical connection** quality and packet collision: if you have packet loss in your data infrastructure, you're probably not ready for VoIP. Network latency and jitter should be minimal. All bottlenecks in the communications will immediately be revealed when VoIP is introduced, even if those weren't readily apparent with traditional data communications.

Attack Examples

Caller-ID spoofing
Presence Hijacking
Eavesdropping

Attacks - Spoofing Caller-ID

Companies that offer Caller-ID Spoofing

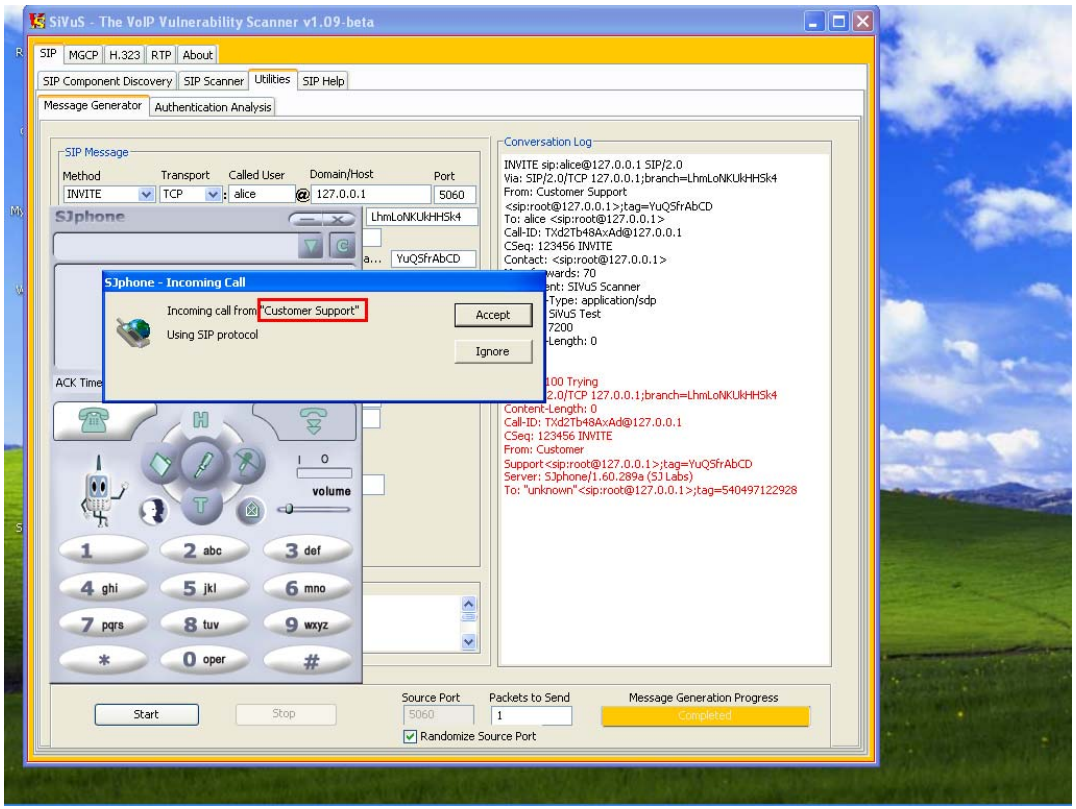
https://connect.voicepulse.com/

http://www.nufone.net/

http://www.spooftel.net/

Spoofing Caller-ID using SiVuS

- Manipulate the FROM header information
- Send and INVITE to a phone



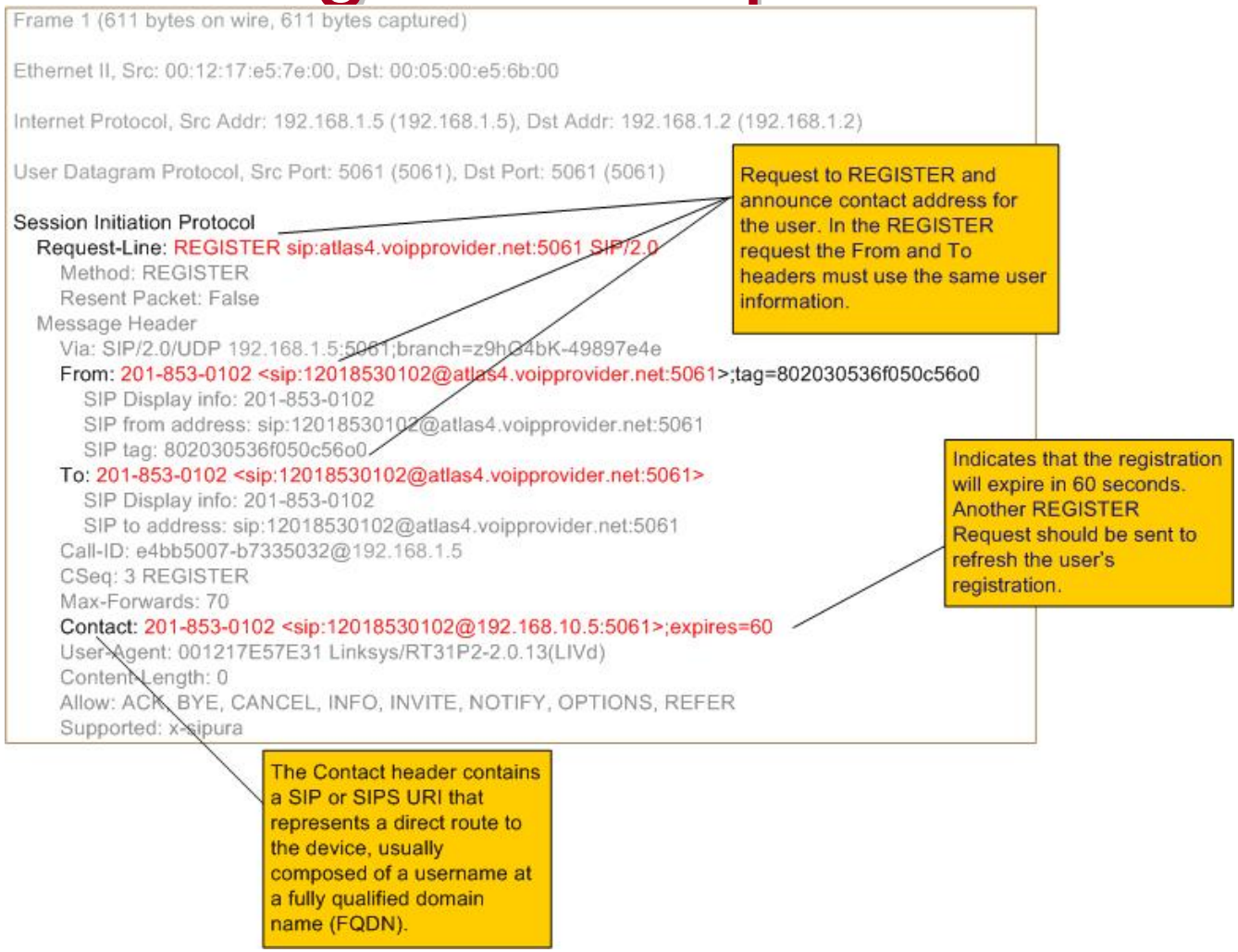
Attacks - Presence Hijacking

Presence Hijacking/Masquerading Attack using SIP

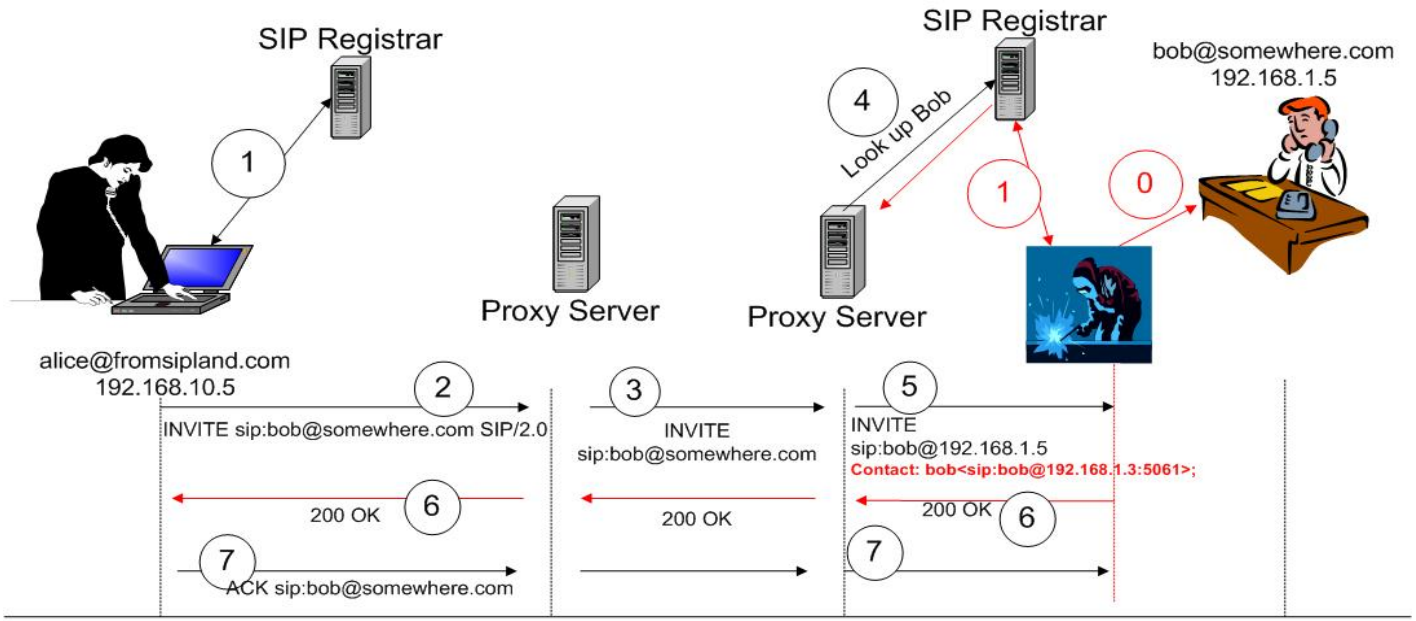
Presence Hijacking using SiVuS

- The objective is to spoof a REGISTER request
- The REGISTER request contains the “Contact:” header which indicates the IP address of the SIP device.

Presence Hijacking using SiVuS – Regular Register Request



The Attack



0 – DoS Attack
1 – User Registration
2 – Caller - Session Initiation Request
3 – Proxy - Domain look up and routing
4 – Proxy - user lookup (SIP Proxy retrieves the attacker's IP address)
5 – Proxy - Proxy contacts user
6 – Calee answers
7 – Proxy forwards caller response – The connection has been established and media is routed between the two phones.

Manipulated REGISTER request properties

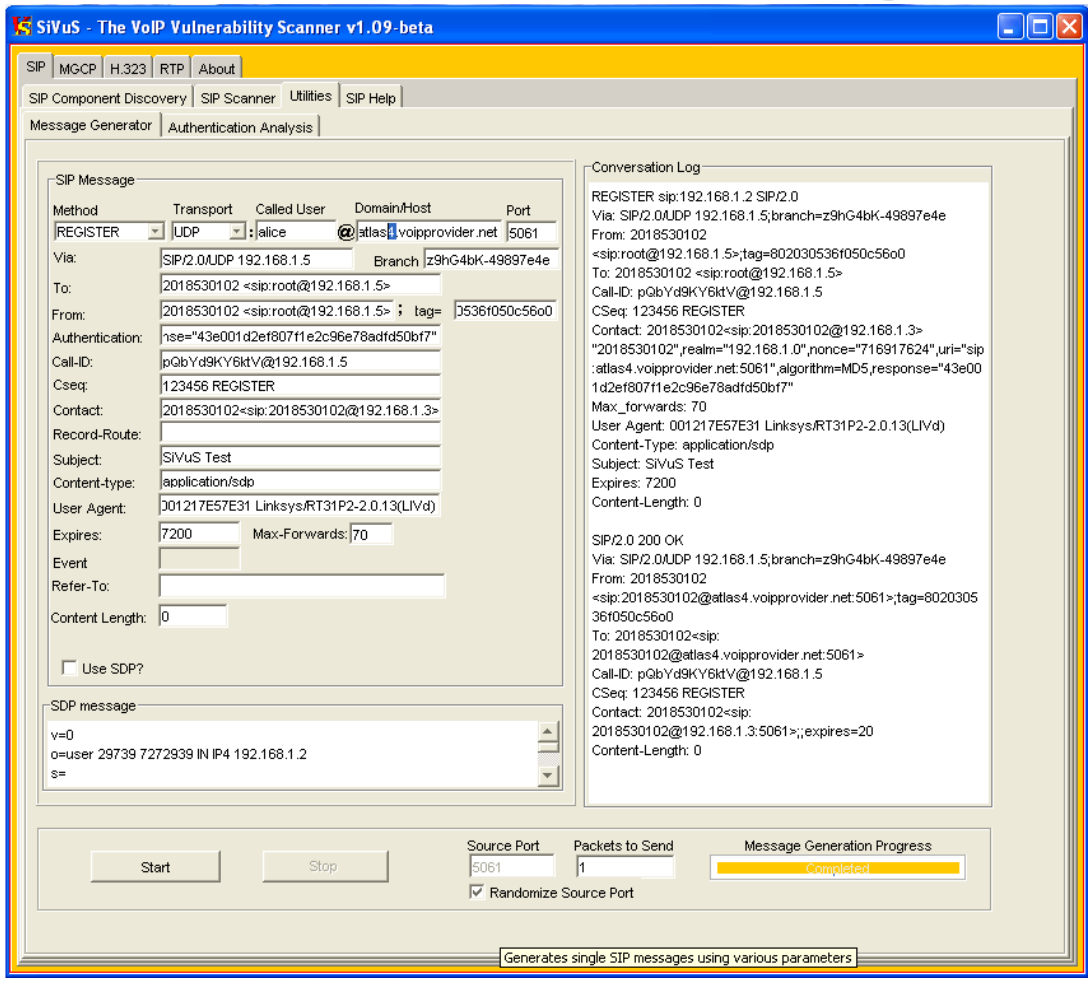
IP address of the VoIP device on which a POTS phone is attached

REGISTER sip:216.1.2.5 SIP/2.0
Via: SIP/2.0/UDP **192.168.1.6**;branch=xajB6FLTEHIcd0
From: 732-835-0102 <sip:12125550102@voip-service-provider.net:5061>;tag=5e374a8bad1f7c5x1
To: 732-835-0102 <sip:12125550102@voip-service-provider.net:5061>
Call-ID: QTEv5G5dOHYc@192.168.1.2
CSeq: 123456 REGISTER
Contact: 2125550102 <sip:12125550102@192.168.1.3:5061>;
Digest username="12125550102",realm="216.1.2.5",nonce="716917624",
uri="sip:voip-service-provider.net:5061",algorithm=MD5,
response="**43e001d2ef807f1e2c96e78adfd50bf7**"
Max_forwards: 70
User Agent: 001217E57E31 VoIP-Router/RT31P2-2.0.13(LIVd)
Content-Type: application/sdp
Subject: SiVuS Test
Expires: 7200
Content-Length: 0

IP address that calls will be routed to (attacker)

Authentication MD5 digest can be intercepted and used to replay messages

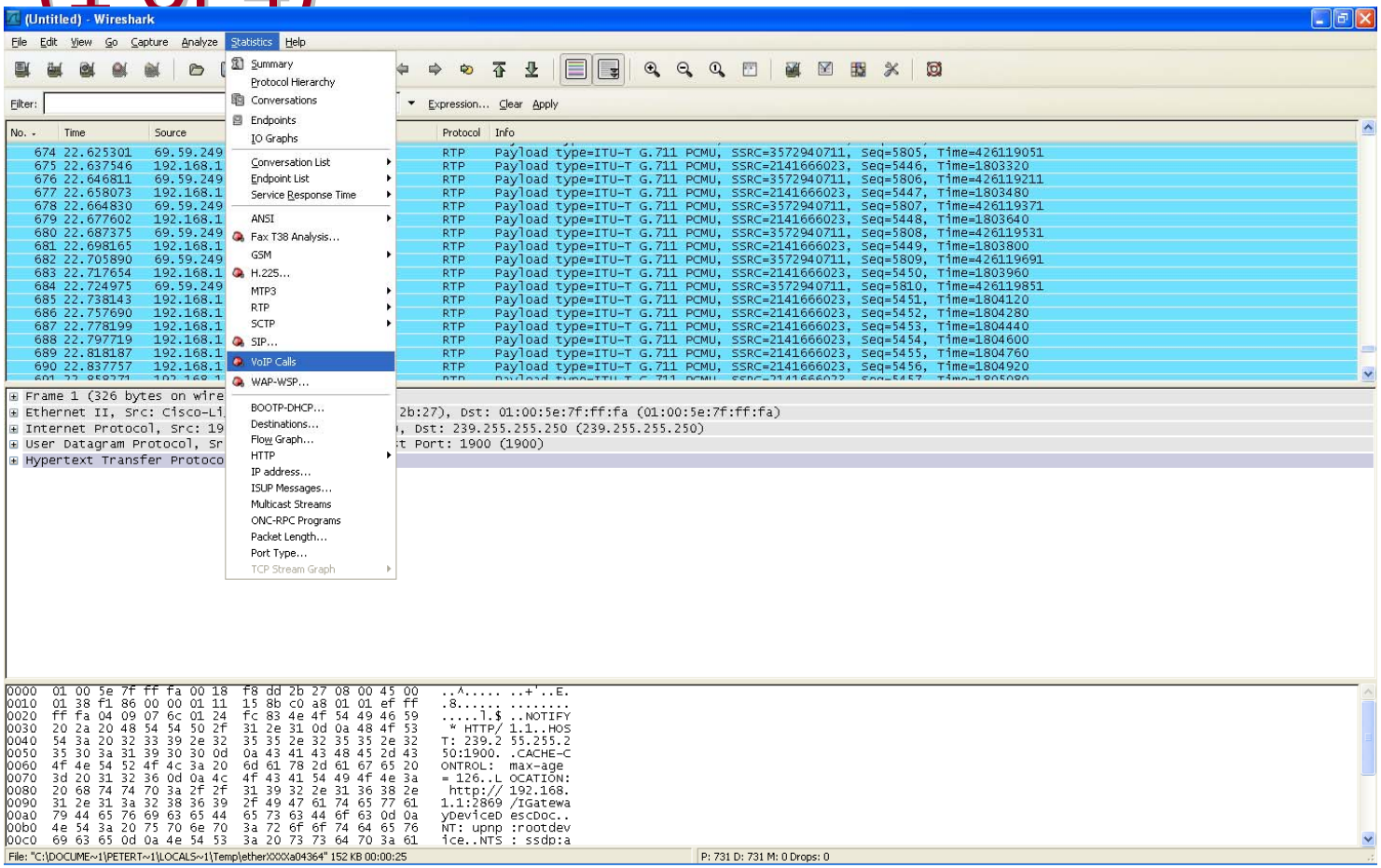
Presence Hijacking using SiVuS – The REGISTER Message



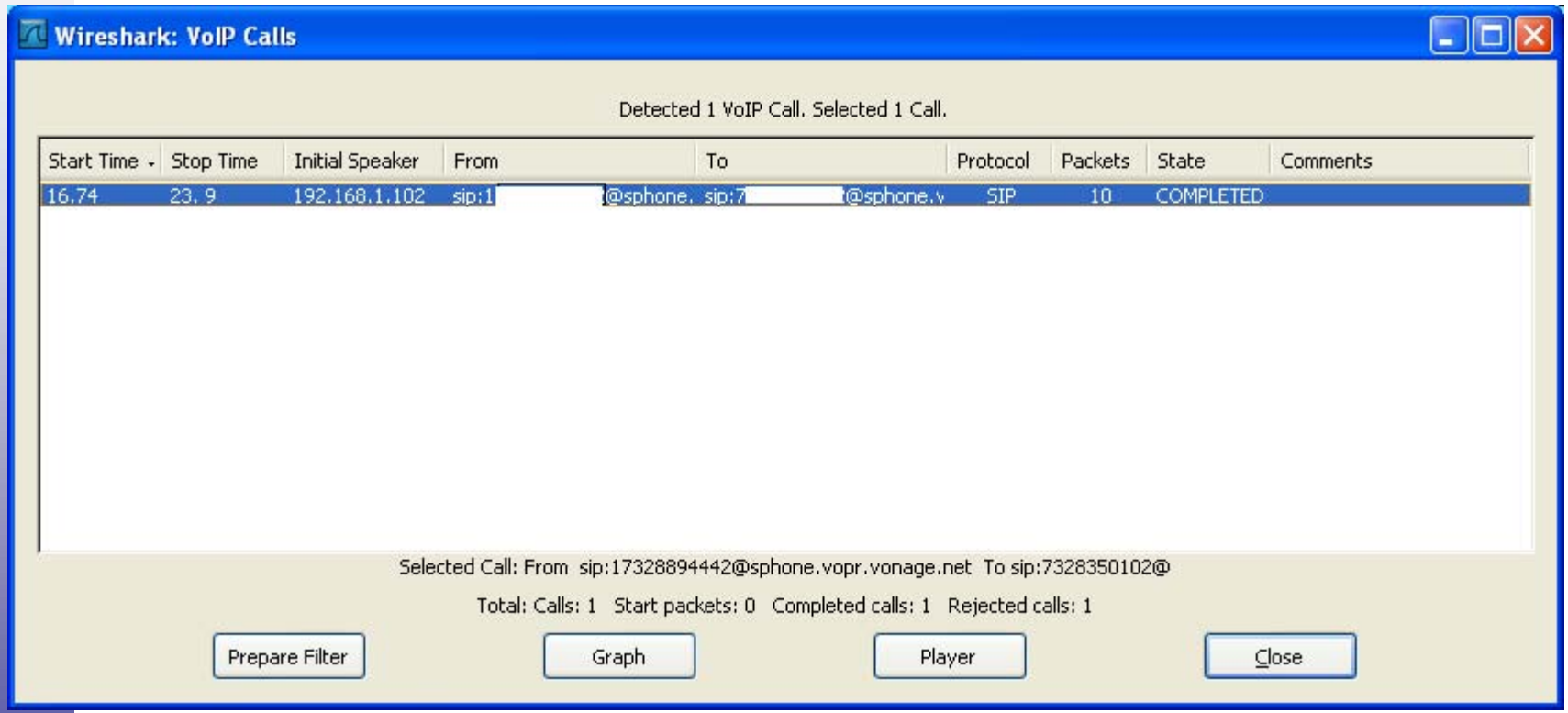
Attacks - Eavesdropping

Decoding communications with Wireshark

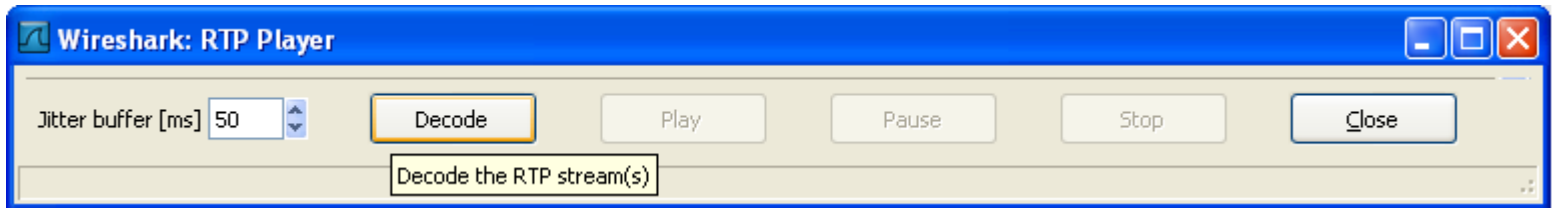
Eavesdropping using Wireshark (1 of 4)



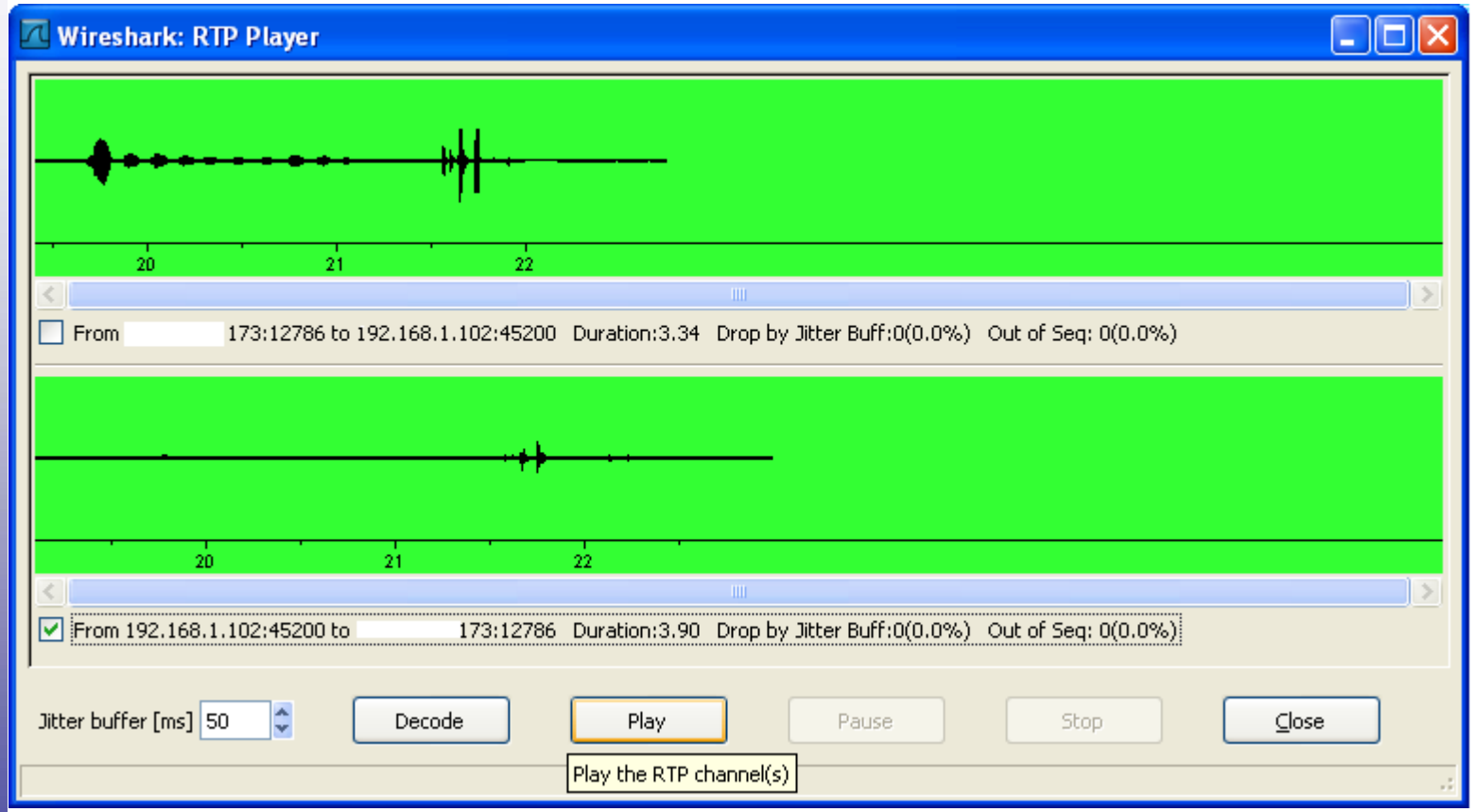
Eavesdroping with Wireshark (2 of 4)



Ethereal capture (3 of 4)



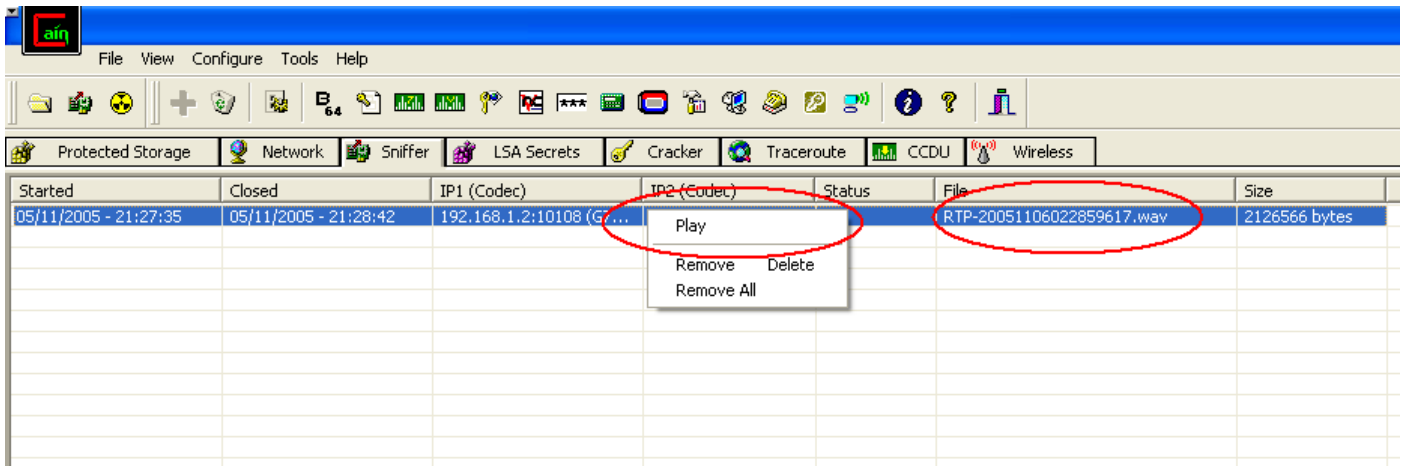
Eavesdropping with Wireshark (4 of 4)



The result

Eavesdropping using Cain & Abel

- Activate the Network Sniffer
- Use ARP spoofing to perform man in the middle attack and capture SIP/RTP traffic

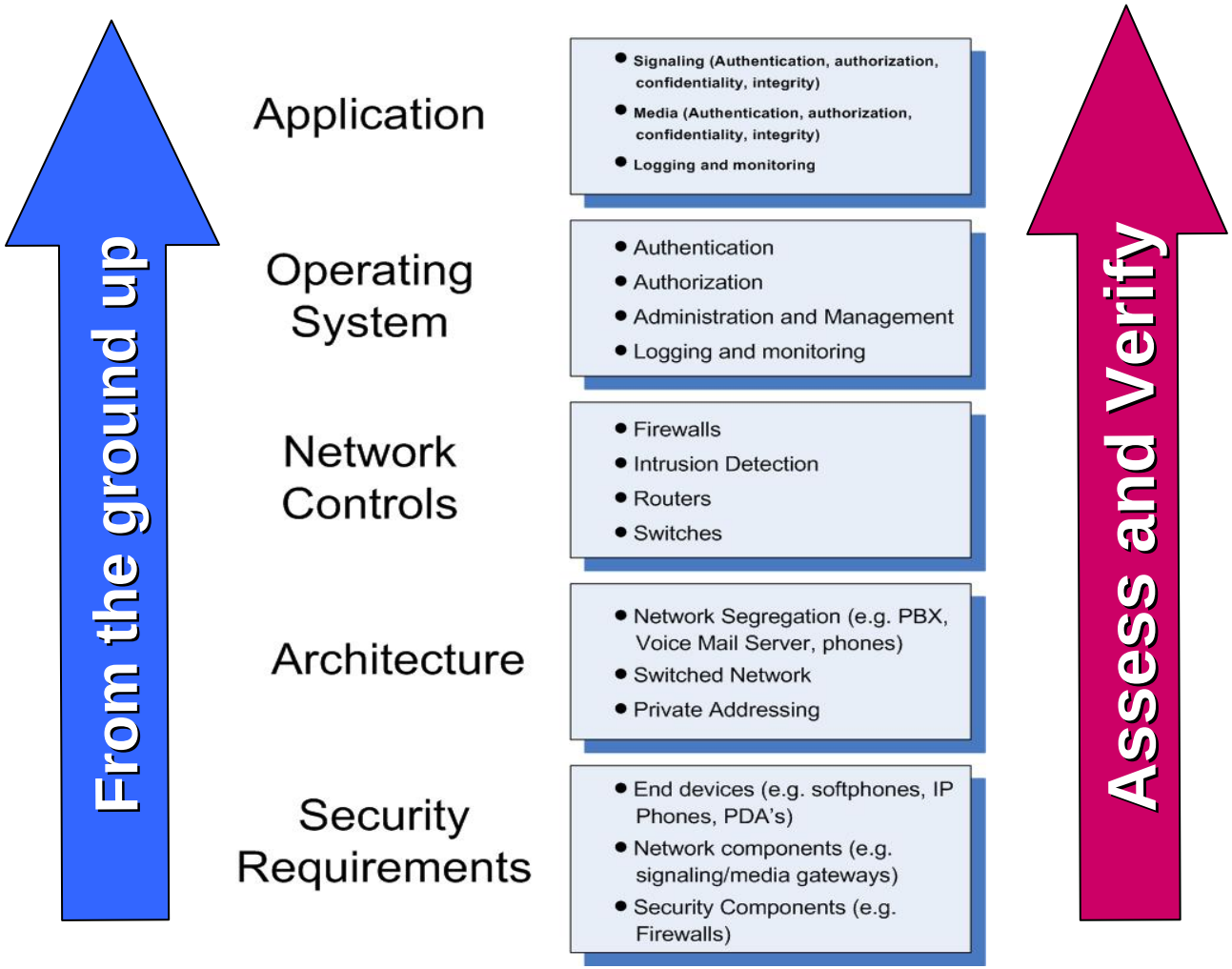


Outline

- Intro – Present and Future
- Components & Protocols
- Security – Threats, Attacks & Vulnerabilities
- **Best Practices**
- Assessment Tools
- Conclusions
- Additional Information for bedtime reading…

Securing VoIP Networks
Best practices

How do we secure VoIP networks?



SECURITY is NOT a product, it's a PROCESS !

VoIP Security Framework

- Policies
- Standards
- Requirements
- Verification
- Vulnerability assessments
  - Methodology
  - Tools

VoIP Security Policy

- Outline in your organizational policy what is the acceptable use of Telecommunications equipment and services
  - Long Distance calling
  - International calling
  - Trunk transfer
  - Forwarding (e.g. an employee forwarding calls to another country)

Standards (1 of 2)

- Define organizational security and reliability standards for VoIP
  - Use of mutual authentication
    - User ← to → device
    - Device ← to → network
  - Use encryption to protect confidentiality of communication
    - Maybe limited to executive personnel

Standards (2 of 2)

- Network Controls
  - Segmentation - VLAN separation
  - Enforcement of ACL's
  - Firewalls/SBC's
  - Intrusion Detection
- Reliability
  - E911 calls should always be routed
  - Define what is the alternative in case of failure
  - Power over Ethernet (PoE)

Requirements

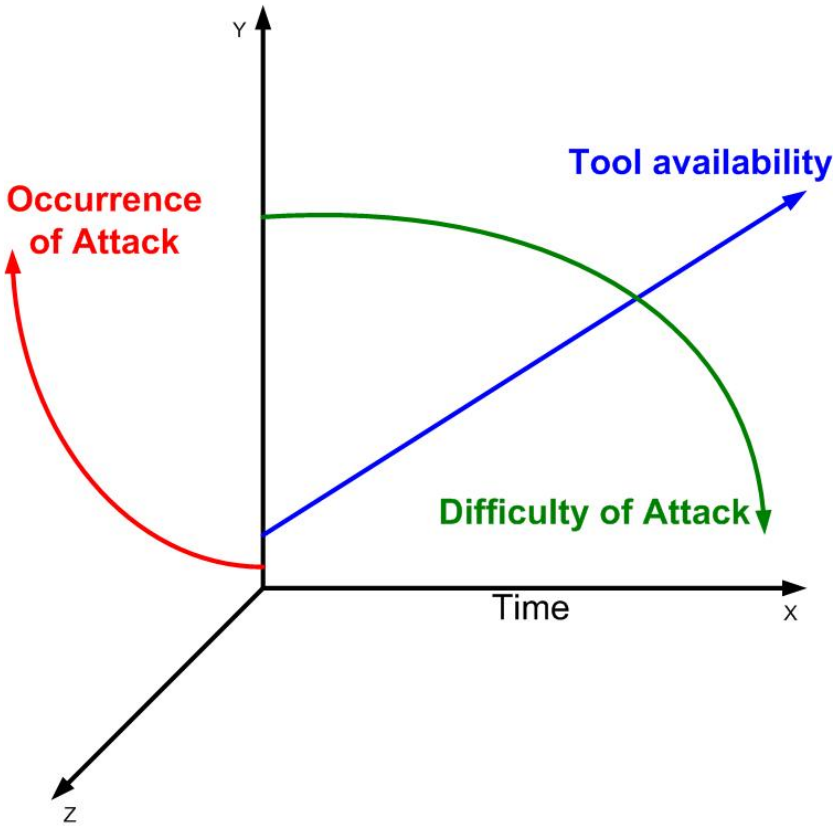
- Security requirements
  - Authentication methods
    - Switch Port Authentication
    - Signaling Message Authentication
  - Network Controls
  - Management and Administration
- Service reliability

Outline

- Intro – Present and Future
- Components & Protocols
- Security – Threats, Attacks & Vulnerabilities
- Best Practices
- **Assessment Tools**
- Conclusions
- Additional Information for bedtime reading…

Tool – Attack Trend

More tools are being developed



VoIP Security Tools – Eavesdropping (1 of 3)

- **Wireshark** - Formerly Ethereal, the premier multi-platform network traffic analyzer. http://www.wireshark.org
- **AuthTool** - Tool that attempts to determine the password of a user by analyzing SIP traffic. http://www.hackingvoip.com/sec_tools.html
- **Cain & Abel** - Multi-purpose tool with the capability to reconstruct RTP media calls. http://www.oxid.it/cain.html
- **Etherpeek-VX** - VoIP sniffer. http://www.wildpackets.com/products/etherpeek/overview

Thanks to Shawn Merdinger and Dustin D. Trammell
http://www.voipsa.org/Resources/tools.php

VoIP Security Tools – Eavesdropping (2 of 3)

- **Oreka** - Oreka is a modular and cross-platform system for recording and retrieval of audio streams. http://oreka.sourceforge.net
- **PSIPDump** - psipdump is a tool for dumping SIP sessions (+RTP traffic, if available) from pcap to disk in a fashion similar to "tcpdump -w". http://sourceforge.net/projects/psipdump
- **SIPomatic** - SIP listener that's part of LinPhone. http://www.linphone.org/?lang=us&rubrique=1
- **VoiPong** - VoIPong is a utility which detects all Voice Over IP calls on a pipeline, and for those which are G711 encoded, dumps actual conversation to separate wave files. It supports SIP, H323, Cisco's Skinny Client Protocol, RTP and RTCP. http://www.enderunix.org/voipong/index.php

VoIP Security Tools – Eavesdropping (3 of 3)

- **VoIPong ISO Bootable** - Bootable "Live-CD" disc version of VoIPong. http://www.enderunix.org/voipong/manual/usage-livecd.html
- **VOMIT** - The vomit utility converts a Cisco IP phone conversation into a wave file that can be played with ordinary sound players. http://vomit.xtdnet.nl
- **NetDude** - A framework for inspection, analysis and manipulation of tcpdump trace files. http://netdude.sourceforge.net

VoIP Security Tools – Scanning and Enumeration (1 of 3)

- **enumIAX** - An IAX2 (Asterisk) login enumerator using REGREQ messages.

  http://sourceforge.net/projects/enumiax/
- **iWar** - IAX2 protocol Wardialer.
  http://www.softwink.com/iwar/
- **SIP Forum Test Framework (SFTF)** - The SIP Forum Test Framework (SFTF) was created to allow SIP device vendors to test their devices for common errors.
  https://www.sipfoundry.org/sftf

VoIP Security Tools – Scanning and Enumeration (2 of 3)

- **SIP-Scan** - A fast SIP network scanner. http://skora.net/voip/voip.html
- **SIPcrack** - SIPcrack is a SIP protocol login cracker. It contains 2 programs, SIPdump to sniff SIP logins over the network and SIPcrack to bruteforce the passwords of the sniffed login. http://remote-exploit.org/index.php/Sipcrack
- **SIPSCAN** - SIPSCAN is a SIP username enumerator that uses INVITE, REGISTER, and OPTIONS methods. http://www.hackingvoip.com/sec_tools.html
- **SiVuS** - A SIP Vulnerability Scanner. http://www.vopsecurity.org/html/tools.html

VoIP Security Tools – Scanning and Enumeration (3 of 3)

- **SMAP** - SIP Stack Fingerprinting Scanner. http://www.wormulon.net/index.php?/archives/1159-smap-0.4.1-released.html
- **VLANping** - VLANPing is a network pinging utility that can work with a VLAN tag. http://www.hackingvoip.com/sec_tools.html
- **VoIPAudit** - VoIP specific scanning and vulnerability scanner. http://www.voipshield.com

Packet generation/Flooding (1 of 2)

- **SIVuS – www.vopsecurity.org**
- **IAXFlooder** - A packet flooder that creates IAX packets. http://www.hackingvoip.com/sec_tools.html
- **INVITE Flooder** - Send a flurry of SIP INVITE messages to a phone or proxy.
- **kphone-ddos** - Using KPhone for flooding attacks with spoofed SIP packets. http://skora.net/voip/voip.html
- RTP Flooder - Creates "well formed" RTP Packets that can flood a phone or proxy. http://www.hackingvoip.com/sec_tools.html
- **Scapy** - Scapy is a powerful interactive packet manipulation program. It can easily handle most classical tasks like scanning, tracerouting, probing, unit tests, attacks or network discovery. http://www.hackingvoip.com/sec_tools.html

Packet generation/Flooding (2 of 2)

- **Seagull** - a multi-protocol traffic generator especially targeted towards IMS. http://gull.sourceforge.net/doc/sip.html
- **SIPBomber** - SIPBomber is sip-protocol testing tool for Linux. http://www.metalinkltd.com/downloads.php
- **SIPNess** - SIPness Messenger is a SIP testing tool which is used for testing SIP applications. http://www.ortena.com/files/Messenger.zip
- **SIPp** - SIPp is a free Open Source test tool / traffic generator for the SIP protocol. http://sipp.sourceforge.net
- **SIPsak** - SIP swiss army knife. http://sipsak.org

Fuzzing Tools (1 of 3)

- **SIVuS** – www.vopsecurity.org
- **Asteroid** - this is a set of malformed SIP methods (INVITE, CANCEL, BYE, etc.) that can be crafted to send to any phone or proxy. http://www.infiltrated.net/asteroid/
- **Codenomicon VoIP Fuzzers** - Commercial versions of the free PROTOS toolset. http://www.codenomicon.com/products/telecommunications/
- **Spirent ThreatEx** - a commercial protocol fuzzer and ribustness tester. http://www.spirentcom.com/general/docview.cfm?D=4663

Fuzzing Tools (2 of 3)

- **Fuzzy Packet** - Fuzzy packet is a tool to manipulate messages through the injection, capturing, receiving or sending of packets generated over a network. Can fuzz RTP and includes built-in ARP poisoner. http://libresource.inria.fr/projects/VoIP_Security/fuzzypacket
- **Mu Security VoIP Fuzzing Platform** - Fuzzing platform handling SIP, H.323 and MGCP protocols. http://www.musecurity.com/products/protocol_usecase.html#voip
- **SIP-Proxy** - Acts as a proxy between a VoIP UserAgent and a VoIP PBX. Exchanged SIP messages pass through the application and can be recorded, manipulated, or fuzzed. http://sourceforge.net/projects/sipproxy

Fuzzing Tools (3 of 3)

- **ohrwurm** - ohrwurm is a small and simple RTP fuzzer. http://mazzoo.de/blog/2006/08/25#ohrwurm
- **PROTOS H.323 Fuzzer** - a java tool that sends a set of malformed H.323 messages designed by the University of OULU in Finland. http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/h2250v4/index.html#download
- **PROTOS SIP Fuzzer** - a java tool that sends a set of malformed SIP messages designed by the University of OULU in Finland. http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/

Signaling Manipulation Tools (1 of 2)

- **SIVuS – www.vopsecurity.org**
- **BYE Teardown** - This tool attempts to disconnect an active VoIP conversation by spoofing the SIP BYE message from the receiving party. http://www.hackingvoip.com/sec_tools.html
- **Check Sync Phone Rebooter** - Transmits a special NOTIFY SIP message which will reboot certain phones. http://www.hackingvoip.com/sec_tools.html
- **RedirectPoison** - this tool works in a SIP signaling environment, to monitor for an INVITE request and respond with a SIP redirect response, causing the issuing system to direct a new INVITE to another location. http://www.hackingvoip.com/sec_tools.html

Signaling Manipulation Tools (2 of 3)

- **Registration Eraser** - this tool will effectively cause a denial of service by sending a spoofed SIP REGISTER message to convince the proxy that a phone/user is unavailable. http://www.hackingvoip.com/sec_tools.html
- **Registration Hijacker** - this tool tries to spoof SIP REGISTER messages in order to cause all incoming calls to be rerouted to the attacker. http://www.hackingvoip.com/sec_tools.html
- **SIP-Kill** - Sniff for SIP-INVITEs and tear down the call. http://skora.net/voip/voip.html

Signaling Manipulation Tools (3 of 3)

- **SIP-Proxy-Kill** - Tears down a SIP-Session at the last proxy before the opposite endpoint in the signaling path. http://skora.net/voip/voip.html
- **SIP-RedirectRTP** - Manipulate SDP headers so that RTP packets are redirected to an RTP-proxy. http://skora.net/voip/voip.html
- **SipRogue** - a multifunctional SIP proxy that can be inserted between two talking parties. http://www.hackingvoip.com/sec_tools.html
- **Registration Adder** - this tool attempts to bind another SIP address to the target, effectively making a phone call ring in two places (the legitimate user's desk and the attacker's). http://www.hackingvoip.com/sec_tools.html

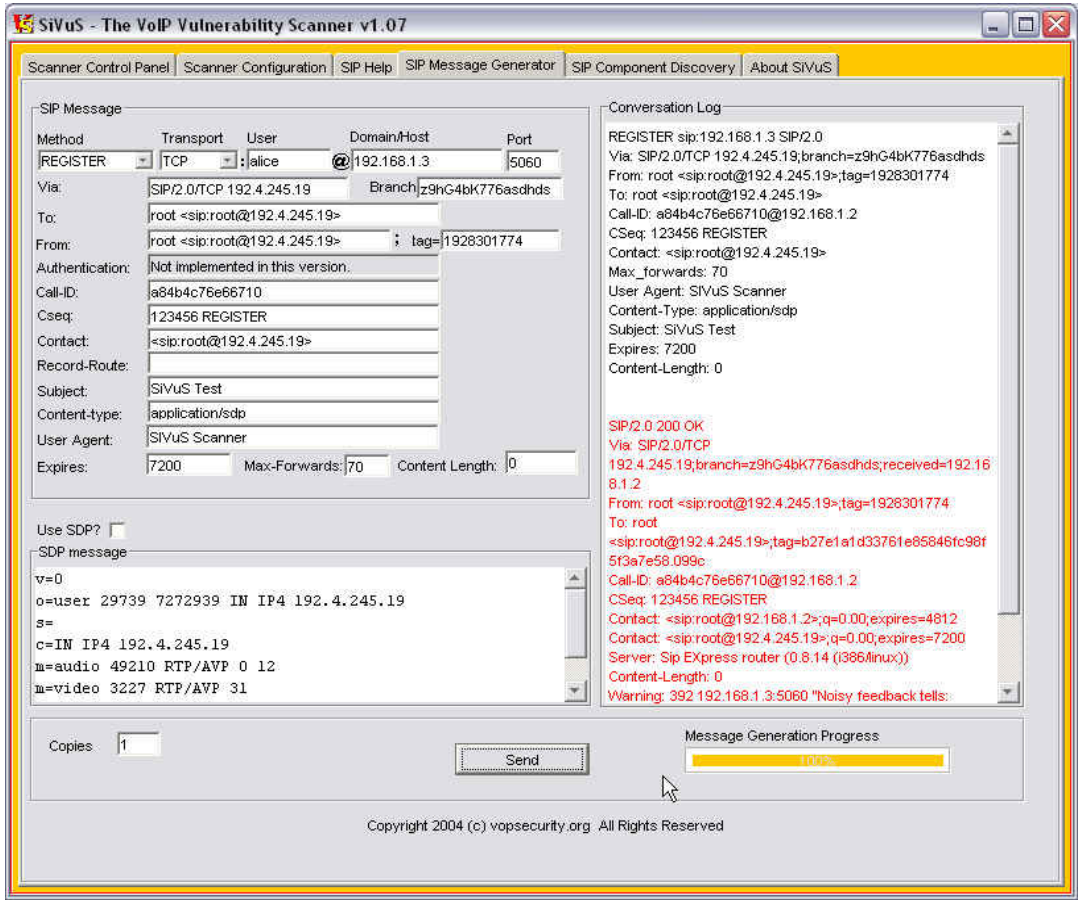
Media Manipulation Tools

- **RTP InsertSound** - this tool takes the contents of a .wav or tcpdump format file and inserts the sound into an active conversation. http://www.hackingvoip.com/sec_tools.html
- **RTP MixSound** - this tool takes the contents of a .wav or tcpdump format file and mixes the sound into an active conversation. http://www.hackingvoip.com/sec_tools.html
- **RTPProxy** - Wait for incoming RTP packets and send them to wanted (signaled by a tiny protocol) destination. http://skora.net/voip/voip.html
- **RAT (Robust Audio Tool).** http://www-mice.cs.ucl.ac.uk/multimedia/software/rat/

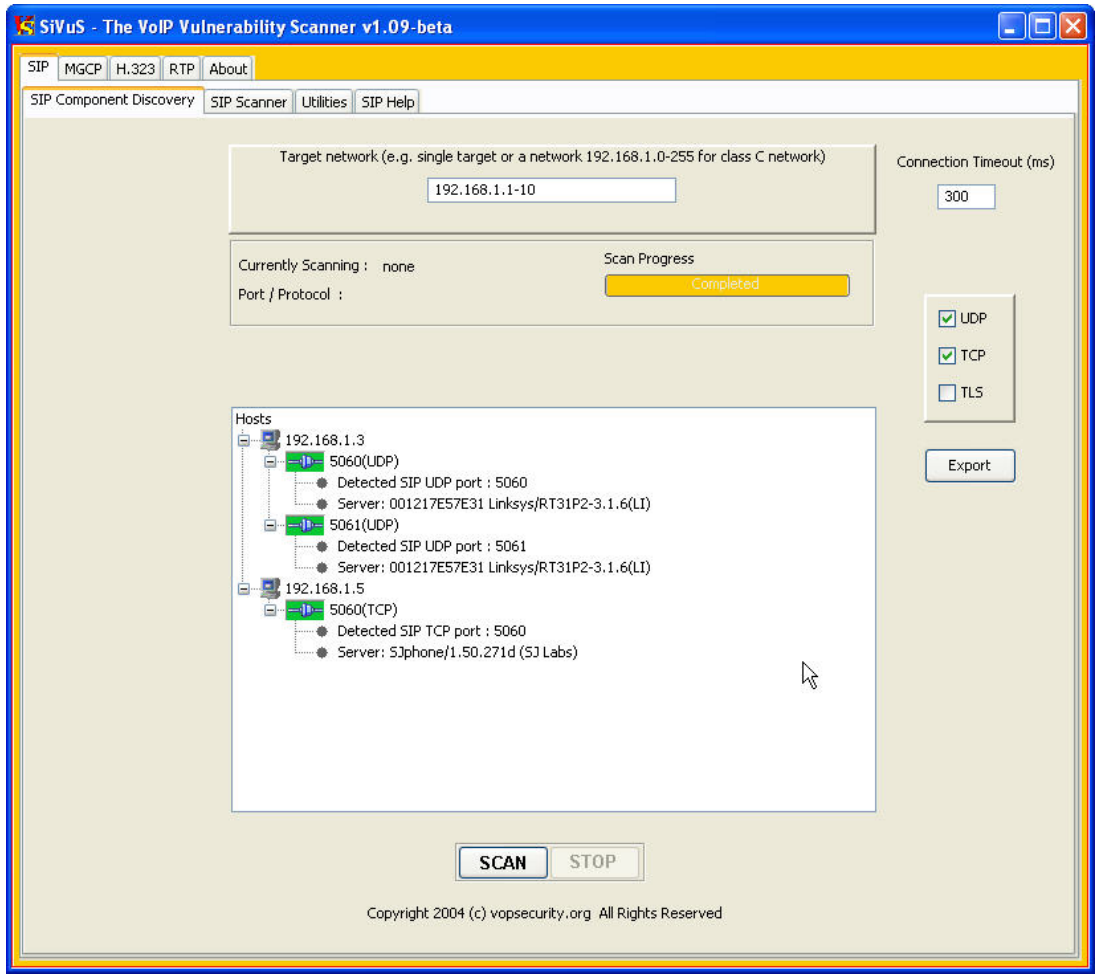
Vulnerability Assessment with SiVuS

SiVuS

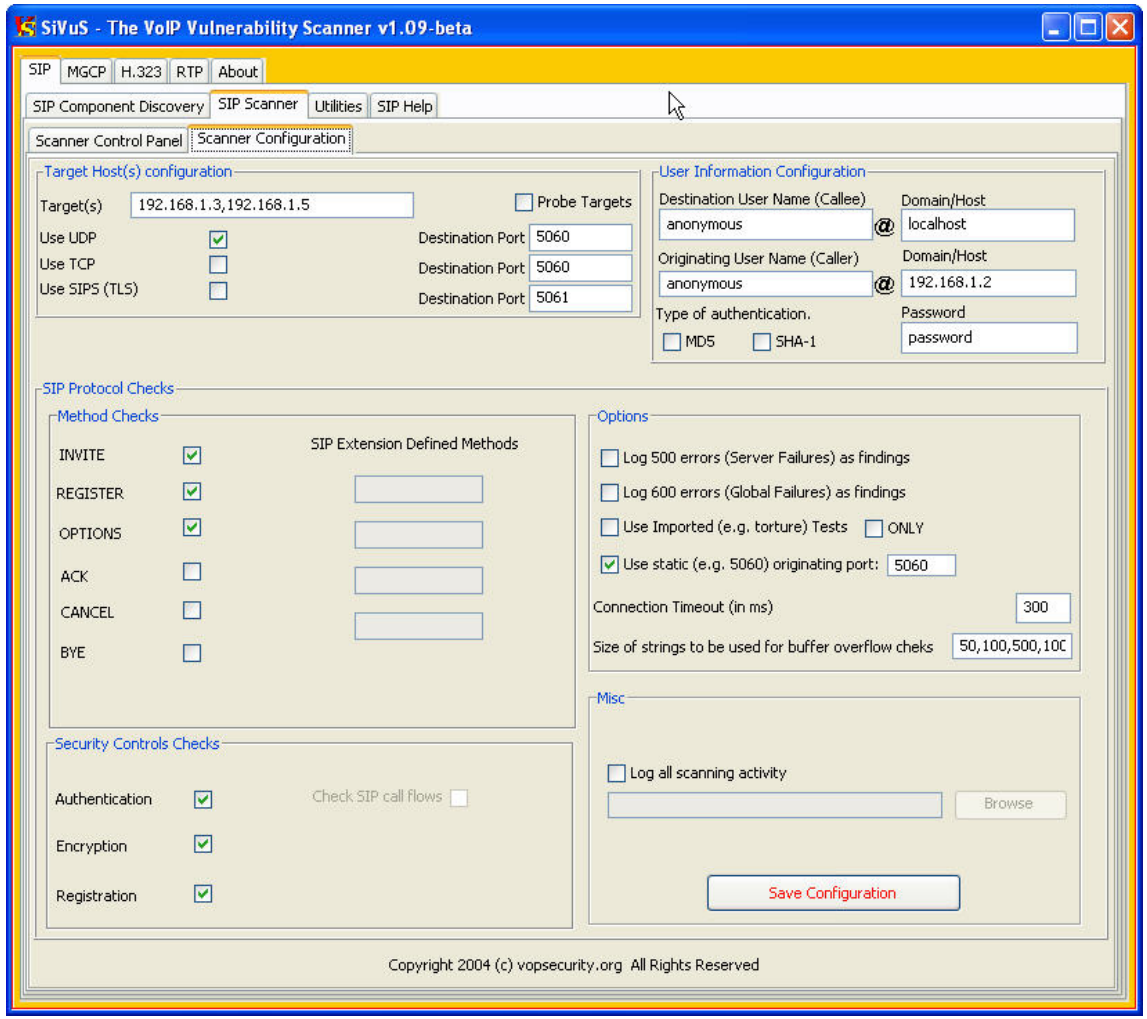
SiVuS – Message Generator



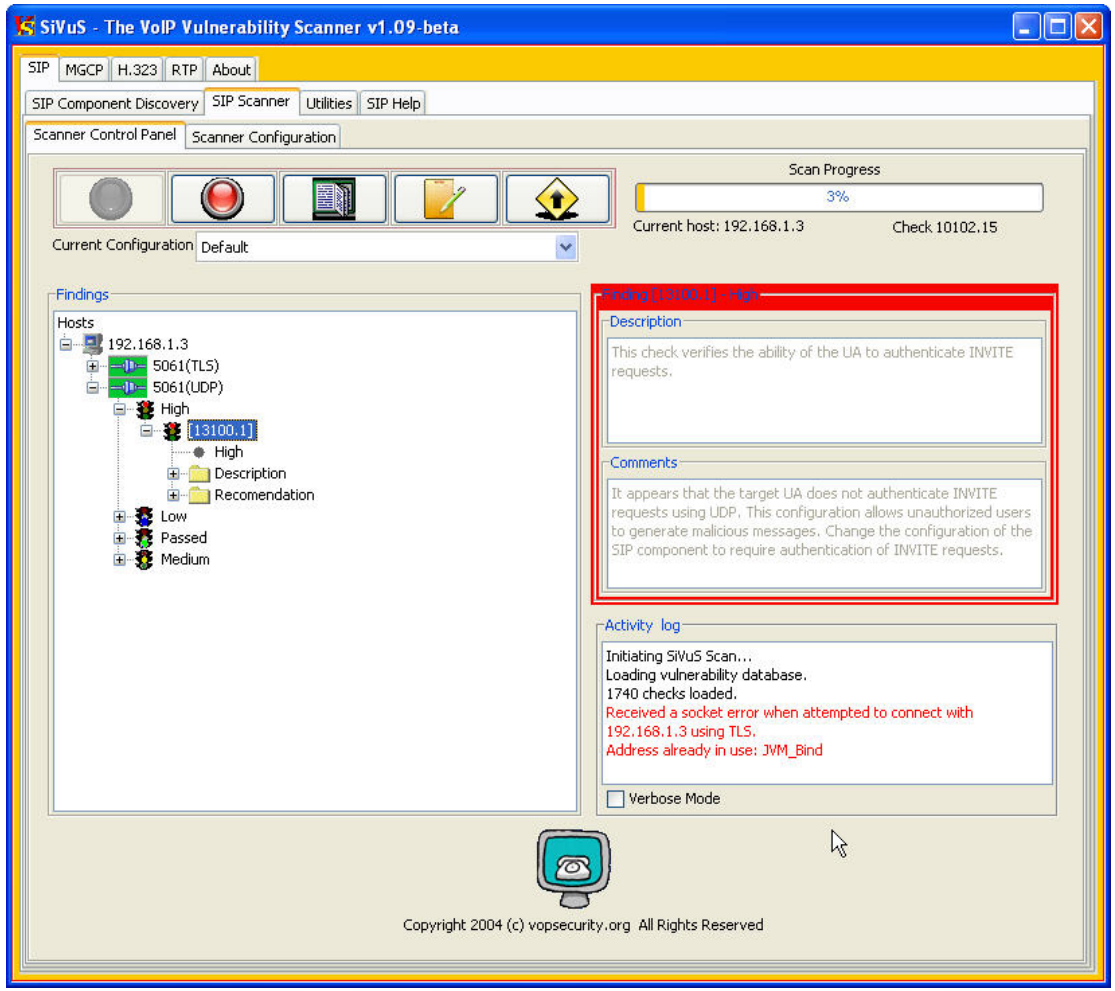
SiVuS - Discovery



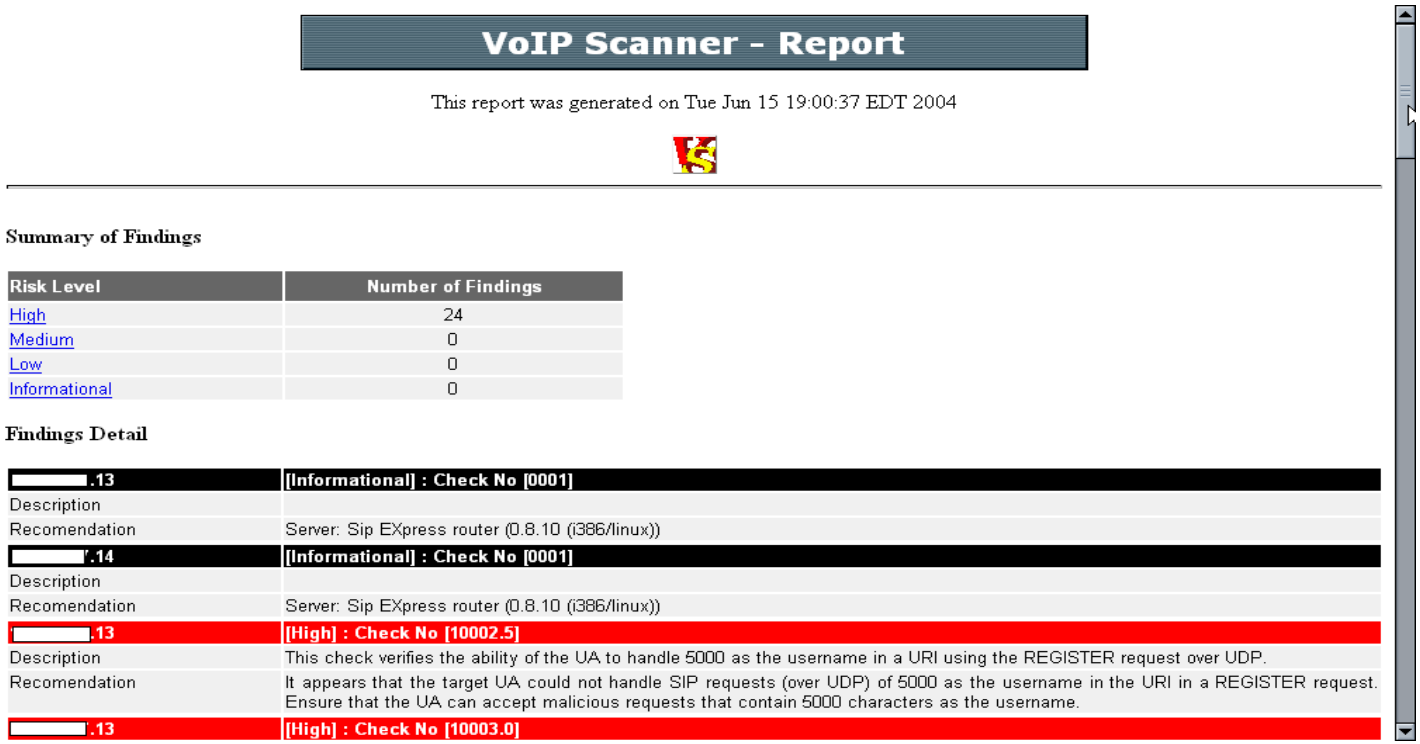
SiVuS – configuration



SiVuS – Control Panel



SiVuS – Reporting



VoIP Scanner - Report

This report was generated on Tue Jun 15 19:00:37 EDT 2004

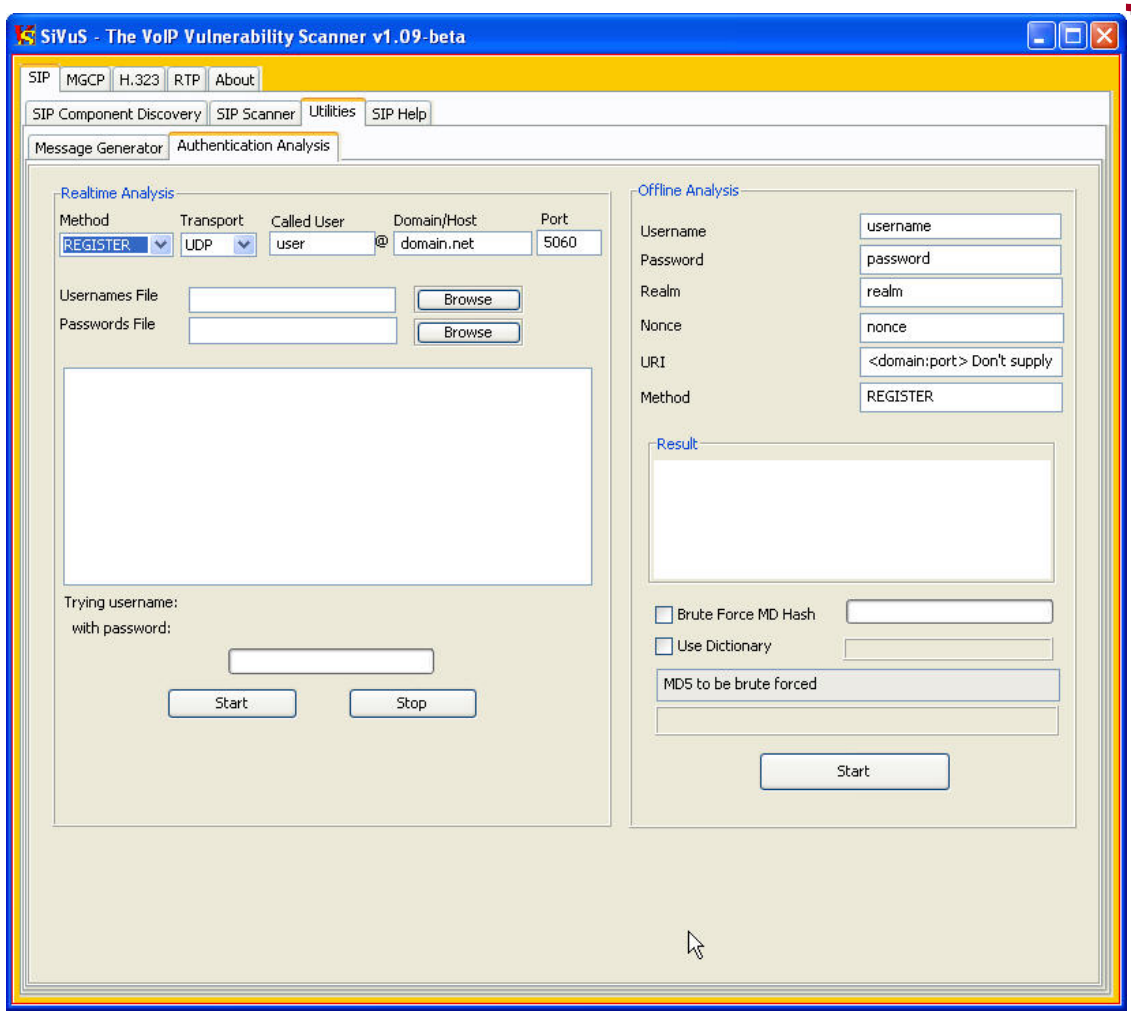
Summary of Findings

Risk Level	Number of Findings
High	24
Medium	0
Low	0
Informational	0

Findings Detail

[redacted].13	[Informational] : Check No [0001]
Description	
Recomendation	Server: Sip EXpress router (0.8.10 (i386/linux))
[redacted].14	[Informational] : Check No [0001]
Description	
Recomendation	Server: Sip EXpress router (0.8.10 (i386/linux))
[redacted].13	[High] : Check No [10002.5]
Description	This check verifies the ability of the UA to handle 5000 as the username in a URI using the REGISTER request over UDP.
Recomendation	It appears that the target UA could not handle SIP requests (over UDP) of 5000 as the username in the URI in a REGISTER request. Ensure that the UA can accept malicious requests that contain 5000 characters as the username.
[redacted].13	[High] : Check No [10003.0]

SiVuS – Authentication Analysis



Outline

- Intro – Present and Future
- Components & Protocols
- Security – Threats, Attacks & Vulnerabilities
- Best Practices
- Assessment Tools
- **Conclusions**
- Additional Information for bedtime reading…

Conclusions

Return to the PSTN…

Just kidding…

Conclusions

- VoIP can be a secure and reliable service
- Identify your security requirements early
- If you integrate security in your initial design you will:
  - Alleviate the perceived cost of security as an "added" expense rather as "inherent property of the service"!
  - Establish the foundation to adopt to new security threats
- Test, test, test

Outline

- Intro – Present and Future
- Components & Protocols
- Security – Threats, Attacks & Vulnerabilities
- Best Practices
- Assessment Tools
- Conclusions
- **Additional Information for bedtime reading…**

References

- VoIPSA – VoIP Security Alliance, www.voipsa.org
- The VoP Security Forum, www.vopsecurity.org
- NIST –
  - Security Considerations for VoIP Systems
  - Voice over Internet Protocol (VoIP), Security Technical Implementation Guide (DISA)
- http://www.ietf.org/html.charters/iptel-charter.html
- IP Telephony Tutorial, http://www.pt.com/tutorials/iptelephony/
- Signaling System 7 (SS7), http://www.iec.org/online/tutorials/ss7/topic14.html
- SIP - http://www.cs.columbia.edu/sip/
- IP Telephonly with SIP - www.iptel.org/sip/
- SIP Tutorials
  - The Session Initiation Protocol (SIP)
  - http://www.cs.columbia.edu/~hgs/teaching/ais/slides/sip_long.pdf
  - SIP and the new network communications model http://www.webtorials.com/main/resource/papers/nortel/paper19.htm
- H.323 ITU Standards, http://www.imtc.org/h323.htm
- Third Generation Partnership Project (3gpp), http://www.3gpp.org/

Standards

- ITU
  - Focus Group on Next Generation Networks (FGNGN) - http://www.itu.int/ITU-T/ngn/fgngn/
  - Open Communications Architecture Forum (OCAF) Focus Group http://www.itu.int/ITU-T/ocaf/index.html
- IETF
  - Transport area - http://www.ietf.org/html.charters/wg-dir.html#Transport%20Area
  - Security Area - http://www.ietf.org/html.charters/wg-dir.html#Security%20Area
- ATIS - http://www.atis.org/0191/index.asp
  - T1S1.1--Lawfully Authorized Electronic Surveillance
  - T1S1.2--Security
- Lawful Intercept
  - 3GPP - TS 33.106 and TS 33.107
  - ETSI DTS 102 v4.0.4

VoP Security Forum

Voice over Packet Security Forum

Your single (open) source for NGN/VoIP Security issues and solutions

The **objectives** of the VoPSecurity.org forum:

- Encourage education in NGN/VoIP security through publications, online forums and mailing lists (voptalk@vopsecurity.org and members@vopsecurity.org)
- Develop capabilities (tools, interoperability testing, methodologies and best practices) for members to maintain security in their respective infrastructure.
- Conduct research to help identify vulnerabilities and solutions associated with NGN/VoIP.
- Coordinate annual member meetings to disseminate information, provide updates and promote interaction and initiatives regarding NGN/VoIP security.

The VoP Security forum is viewed as a mechanism for participating members to be proactive and stay current with the threats and vulnerabilities associated with NGN/VoIP security and extend research in this area.

VoPSecurity Forum

Join the community !

- Current Activities
  - Mailing lists
    - Public (voptalk@vopsecurity.org)
  - Documentation
    - Intro to NGN Security (available)
    - Vulnerability Analysis Methodology for VoIP networks (in development)
    - VoIP Firewalls (in development)
  - Tools
    - SiVuS – VoIP vulnerability Scanner (available)
  - Research
    - Security evaluation of residential VoIP gateways

Q & A

Contact info:
Peter Thermos
pthermos@palindrometech.com
Tel: 732 688 0413