CSI 2007

VoIP Attacks!

Dustin D. Trammell
Security Research
BreakingPoint Systems, Inc.
Computer Academic Underground

CSI COMPUTER SECURITY INSTITUTE

About Me

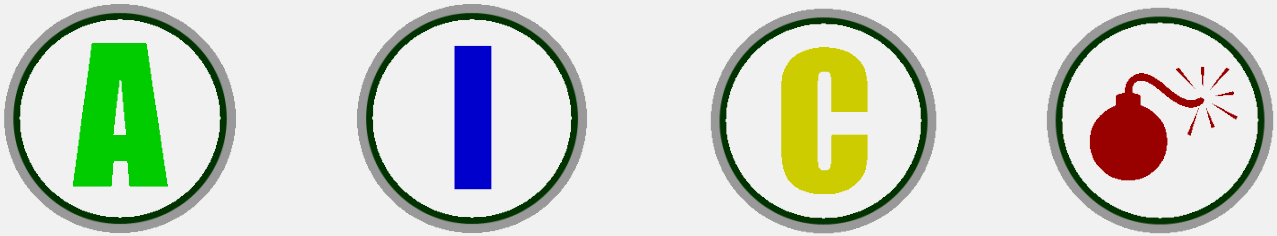
- Dustin D. Trammell a.k.a. I)ruid
- Employed by BreakingPoint Systems, Inc.
  - http://www.bpointsys.com
- Founder, Computer Academic Underground
  - http://www.caughq.org/
- Co-Founder, AHA! (Austin Hackers Association)
  - http://www.austinhackers.org/
- Contributor, VoIP Security Alliance
  - http://www.voipsa.com/

About this Presentation

- Attacks discussed are either recent or significant
- Making the case that attack tools are available *and* mature
- Divided into three sections:
  - Briefly, VoIP Basics
  - Attacks (Vulns, Attacks, Impact, Tools, Mitigation)
  - Problems with suggested mitigation actions
- I'll be discussing only technical attacks

Legend

- Attack Classes
  - Attack against Availability
  - Attack against Integrity
  - Attack against Confidentiality
- Currently Un-patched
- Example / Demo
- Attack Tool References



Notes on Mitigation

- Often there are no clear-cut “solutions” to any vulnerability or attack
- I will refrain from using the “isolate your VoIP network” cop-out “solution”
- Some mitigation techniques suggested do work; In part three, I’ll only be discussing:
  - Those that don’t work well
  - Those that have significant drawbacks
  - Those that have significant barriers to implementation

VoIP Basics

VoIP for the uninitiated...

Terminology

- VoIP - Voice over Internet Protocol
- Call - the session aggregate of signaling and media between endpoints
- Endpoint - Point where a call terminates
- Soft-phone - VoIP phone implemented entirely in software
- Hard-phone - VoIP phone with a physical presence, also sometimes referred to as a “handset”
- PSTN - Public Switched Telephone Network, or your traditional telephony networks.

Signaling vs. Media

- Separate channels for signaling information vs. media (bearer) data due to abuse
- Adopted from traditional telephony systems
- Some protocols like IAX/IAX2 combine these into a single channel

Protocols & Ports

- Signaling
  - Session Initiation Protocol (SIP) : TCP/UDP 5060,5061
  - Session Description Protocol (SDP) : Encapsulated in SIP
  - Media Gateway Control Protocol (MGCP) : UDP 2427,2727
  - Skinny Client Control Protocol (SCCP/Skinny) : TCP 2000,2001
  - Real-time Transfer Control Protocol (RTCP) : (S)RTP+1
- Media
  - Real-time Transfer Protocol (RTP) : Dynamic
  - Secure Real-time Transfer Protocol (SRTP) : Dynamic
- Hybrid
  - Inter-Asterisk eXchange v.1 (IAX): UDP 5036 (obsolete)
  - Inter-Asterisk eXchange v.2 (IAX2) : UDP 4569

H.323 Protocol Suite & Ports

- Signaling
  - H.245 - Call Parameters - Dynamic TCP
  - H.225.0
    - Q.931 - Call Setup - TCP 1720
    - RAS - UDP 1719
  - Audio Call Control - TCP 1731
  - RTCP - RTP Control - Dynamic UDP
- Media
  - RTP - Audio - Dynamic UDP
  - RTP - Video - Dynamic UDP

Audio Codecs

- DoD CELP - 4.8 Kbps
- GIPS Family - 13.3 Kbps and up
- iLBC - 15 Kbps, 20ms frames / 13.3 Kbps, 30ms frames
- ITU G.711 - 64Kbps (a.k.a. alaw / ulaw)
- ITU G.722 - 48 / 56 / 64 Kbps
- ITU G.723.1 - 5.3 / 6.3 Kbps, 30ms frames
- ITU G.726 - 16 / 24 / 32 / 40 Kbps
- ITU G.728 - 16 Kbps
- ITU G.729 - 8 Kbps, 10ms frames
- LPC10 - 2.5 Kbps
- Speex - 2.15 to 44.2 Kbps, Free Open-Source codec
- http://www.voip-info.org/wiki-Codecs

VoIP Attacks!

Generalized Attacks

Flooding

- Vulnerabilities:
  - Most hard-phones have limited or underpowered hardware
  - Protocols provide unauthenticated and unauthorized functions
- Attack:
  - Flood the device with VoIP protocol packets:
    - SIP INVITE, OPTIONS
    - Bogus RTP media packets
  - Flood the device with network protocol packets:
    - TCP SYN
    - ICMP
- Effect:
  - Degraded call quality
  - Device crash, halt, freeze, or respond poorly

Flooding

- Tools:
  - Scapy - General purpose packet tool
    - http://www.secdev.org/projects/scapy/
  - InviteFlood - SIP Invite flooder
    - http://www.hackingexposedvoip.com/tools/inviteflood.tar.gz
  - IAXFlood - IAX protocol flooder
    - http://www.hackingexposedvoip.com/tools/iaxflood.tar.gz
  - UDPFlood - General UDP flooder
    - http://www.hackingexposedvoip.com/tools/udpflood.tar.gz
  - RTPFlood - RTP protocol flooder
    - http://www.hackingexposedvoip.com/tools/rtpflood.tar.gz
- Mitigation:
  - Protect your core network devices from external access
  - Rate-limit VoIP traffic at points of control

Flood Amplification

- Vulnerabilities:
  - Protocols provide unauthenticated functionality
  - Some protocols use a connectionless transport (UDP)
- Attack:
  - Spoof the source address of your packet as originating from your victim
  - Spread the love around
  - Invoke functionality that responds with more data than the request
- Effect:
  - “Smurf”-like amplification flood

Flood Amplification

- Tools:
  - Scapy - General purpose packet tool
    - http://www.secdev.org/projects/scapy/
  - NetSamhain
    - http://sourceforge.net/projects/netsamhain/
  - Nemesis
    - http://www.packetfactory.net/projects/nemesis/
- Mitigation:
  - Use a connection oriented transport (TCP)
  - Authenticate protocol messages
  - Rate-limit network traffic

Fuzzing

- Vulnerabilities:
  - Protocol stack implementations are immature / poor
- Attack:
  - Send malformed messages to a device's input vectors
- Effect:
  - Many endpoint devices will crash, halt, freeze, respond poorly, or otherwise enter a DoS condition
  - Some core devices may behave similarly
  - Very effective method of identifying software bugs

Fuzzing

- Tools:
  - Sulley Fuzzer
    - http://www.fuzzing.org
  - PROTOS Suite - SIP, HTTP, SNMP
    - http://www.ee.oulu.fi/research/ouspg/protos/
  - ohrwurm - RTP
    - http://mazzoo.de/blog/2006/08/25#ohrwurm
  - Fuzzy Packet - RTP, built-in ARP poisoner
    - http://libresource.inria.fr/projects/VoIP_Security/fuzzypacket
  - Other tools
    - http://www.threatmind.net/secwiki/FuzzingTools
- Mitigation:
  - Use open-source soft-phones and hard-phone firmware
  - Demand resilient devices from your device vendor
  - Ask about and review your vendor's QA processes

Attacks Against Signaling

Signaling Manipulation Overview

- Vulnerabilities:
  - Protocols are unencrypted and unauthenticated
  - Signaling extends to endpoint device
- Attacks:
  - Inject malicious signaling messages into a signaling channel
  - Send new signaling messages to endpoints or services
- Effects:
  - Forced call tear-down DoS
  - Media redirection, injection, or call hijacking
  - Registration manipulation DoS / hijack

Forced Call Teardown

- Vulnerabilities:
  - Most protocols are unencrypted and do not authenticate all packets
  - The signaling channel can be monitored
- Attack:
  - Inject spoofed call tear-down messages into the signaling channel such as:
    - SIP: BYE
    - IAX: HANGUP (Frame type 0x06, Subclass 0x05)
- Effect:
  - DoS: A call in progress is forcibly closed.

Forced Call Teardown

- Tools:
  - Teardown - SIP BYE injector
    - http://www.hackingexposedvoip.com/tools/teardown.tar.gz
  - sip-kill - Injects valid SIP teardown messages into a session
    - http://skora.net/uploads/media/sip-kill
  - sip-proxykill - Similar technique against SIP proxies
    - http://skora.net/uploads/media/sip-proxykill
  - IAXHangup
    - http://website.isecpartners.com/files/IAXHangup.tar.gz
  - H225RegReject
    - http://website.isecpartners.com/files/h225regreject.tar.gz
- Mitigation:
  - Encrypt the signaling channel
  - Authenticate every signaling message

Registration (Call) Hijacking

- Vulnerability:
  - Signaling protocols are unencrypted
- Attack:
  - Observe a legitimate endpoint registration
  - Use observed information and credentials to replace the legitimate registration
  - Observe a call-setup message
- Effect
  - New calls for the endpoint are routed to the malicious device rather than the legitimate device

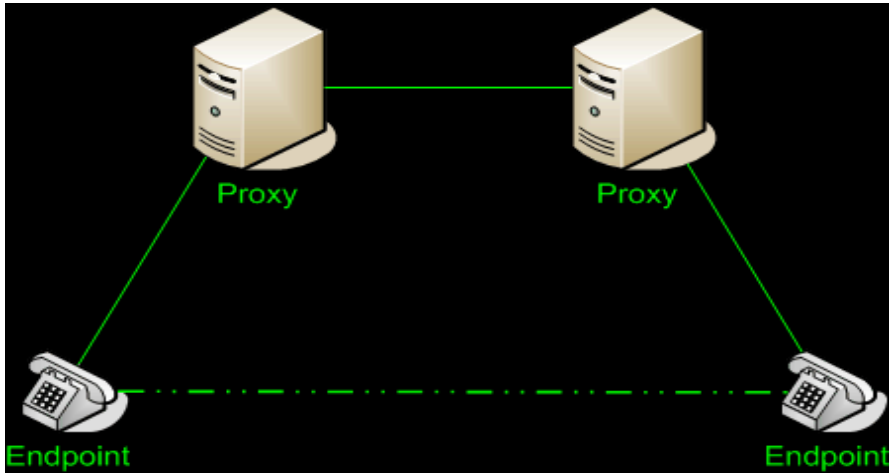
Registration (Call) Hijacking

- Tools
  - Registration Hijacker
    - http://www.hackingexposedvoip.com/tools/reghijacker.tar.gz
  - Registration Remover
    - http://www.hackingexposedvoip.com/tools/eraseregistrations.tar.gz
  - Registration Adder
    - http://www.hackingexposedvoip.com/tools/add_registrations.tar.gz
  - RedirectPoison
    - http://www.hackingvoip.com/tools/redirectpoison_v1.1.tar.gz
- Mitigation
  - Encrypt signaling traffic

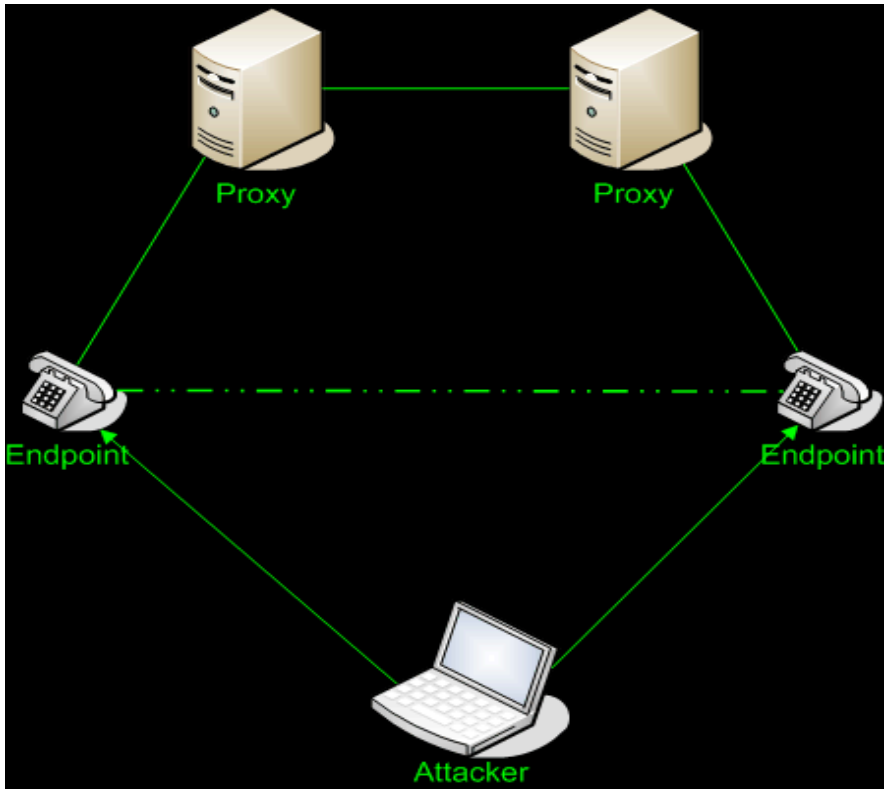
Media Hijacking

- Vulnerabilities:
  - Signaling protocols are unencrypted and unauthenticated
  - Signaling extends to endpoint device
- Attack:
  - Inject malicious signaling messages into a signaling channel
  - Send new signaling messages to endpoints or services
- Effect:
  - Media redirection, duplication, or termination

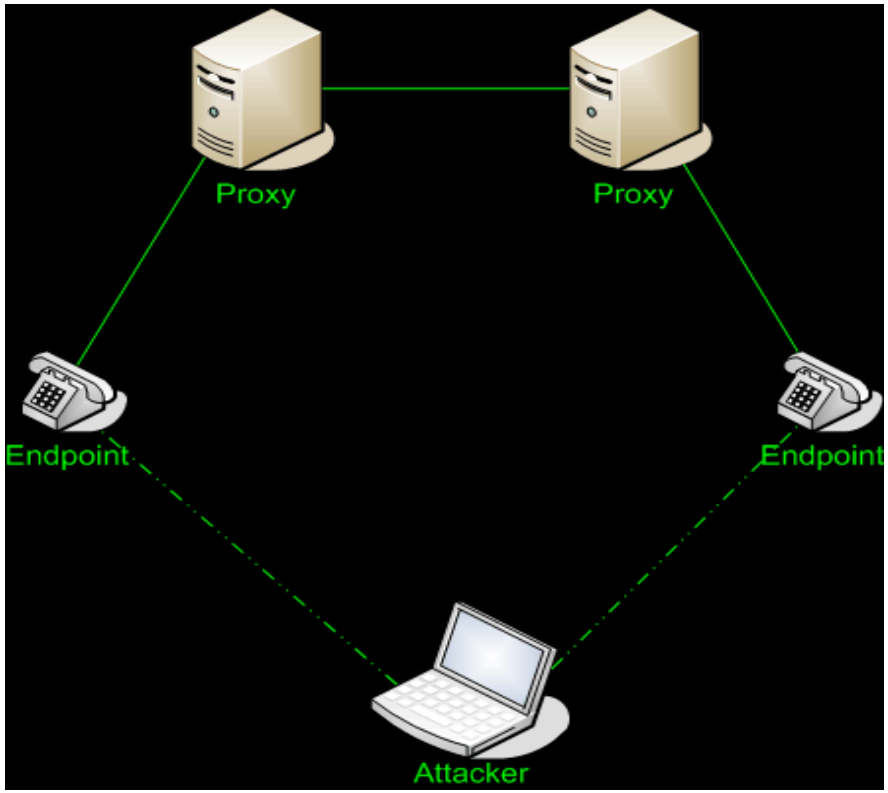
Media Hijacking Example



Media Hijacking Example



Media Hijacking Example



Media Hijacking

- Tools:
  - sip-redirectrtp + rtpproxy
    - http://skora.net/voip/attacks/
- Mitigation:
  - Encrypt the signaling channel
  - Fix protocols to authenticate ALL signaling messages related to a call

Caller-ID Spoofing

- Vulnerability:
  - Protocols are un-authorized and un-verified end-to-end
  - End-point supplied data is not challenged
  - Many automated systems use Caller-ID information to authenticate users
- Attack:
  - Initiate a call with falsified Caller-ID information
- Effect:
  - An attacker may appear to the called party as someone they are not
  - An attacker may be erroneously authenticated

Caller-ID Spoofing

- Tools:
  - Most soft-phones
  - Asterisk IPBX
  - VoIP to PSTN service providers that honor user-supplied Caller-ID information
    - http://www.iax.cc/ - IAX/SIP VoIP Service provider
    - http://www.spoofcard.com/ - Calling-card based
    - http://www.telespoof.com/ - For “business” use
    - http://www.fakecaller.com/ - Text to Voice “prank” messages!
- Mitigation:
  - Don’t honor user-supplied Caller-ID information
  - Don’t trust Caller-ID information for user authentication

Caller-ID Name Disclosure

- Vulnerability:
  - Caller-ID Information can be spoofed
  - PSTN switches add name information to Caller-ID
- Attack:
  - Set your Caller-ID to the number you want to identify
  - Call yourself so that the path of your call routes through the PSTN
  - Receive the Caller-ID information which will have the name associated with the number
- Effect:
  - Phone Number to Name Lookup
  - Disclosure of potentially unlisted information

Caller-ID Name Disclosure

- Tools:
  - Asterisk IPBX
  - Most soft-phones
  - VoIP to PSTN service providers that honor user-supplied Caller-ID information
    - http://www.iax.cc/ - IAX VoIP provider, use Asterisk!
    - http://www.spoofcard.com/ - Calling-card based
    - http://www.telespoof.com/ - For “business” use
    - http://www.fakecaller.com/ - Text to Voice “prank” messages!
  - PSTN Telephone Line w/Caller-ID
- Mitigation:
  - Have the PSTN telephony provider remove the Caller-ID name associated with your number

Eavesdropping the Environment

- Vulnerabilities:
  - Signaling extends to the endpoint devices
  - Signaling is neither authenticated nor encrypted
- Attack:
  - Send malformed call set-up signaling to a device
- Effect:
  - Device silently answer the incoming call
  - Audio from the device's environment may be eavesdropped

Eavesdropping the Environment

- Tools
  - Grandstream GXV-3000 SIP Phone exploit:
    - http://voipsa.org/pipermail/voipsec_voipsa.org/2007-August/002424.html
  - Other undisclosed devices have the same issue
- Mitigation
  - Affected vendors need to patch their protocol stacks
  - Devices with available patches need to be updated

Directory Enumeration

- Vulnerabilities:
  - Protocols provide unauthenticated functionality
  - Protocols respond differently to valid vs. invalid usernames
  - Protocols are unencrypted on the wire
- Attack:
  - Active: Send specially crafted protocol messages which elicit a telling response from the server
  - Passive: Watch network traffic for device registration messages
- Effect:
  - Valid usernames are disclosed
  - Usernames may be used in a more targeted attack such as pass-phrase cracking.

Directory Enumeration Example

- Send this to target SIP device:

```
OPTIONS sip:test@172.16.3.20 SIP/2.0
Via: SIP/2.0/TCP 172.16.3.33;branch=3afGeVi3c92Lfp
To: test <sip:test@172.16.3.20>
Content-Length: 0
```

- Receive:

```
SIP/2.0 404 Not Found
```

Directory Enumeration

- Tools:
  - SIPCrack - Sniffs traffic for valid usernames and then attempts to crack their passwords
    - http://www.remote-exploit.org/index.php/Sipcrack
  - enumIAX - Uses IAX REGREQ messages against Asterisk
    - http://www.tippingpoint.com/security/materials/enumiax-0.4a.tar.gz
  - SIPSCAN - Uses SIP OPTIONS, INVITE, and REGISTER messages against SIP servers
    - http://www.hackingexposedvoip.com/tools/sipscan.msi
- Mitigation:
  - Encrypt signaling to prevent passive enumeration
  - Fix protocols that respond differently to valid vs. invalid username registrations.

Attacks Against the Media

Media Injection

- Vulnerability
  - Media channel packets are unauthenticated and unencrypted
- Attack:
  - Inject new media into an active media channel
  - Replace media in an active media channel
- Effect:
  - Modification of media
  - Replacement of media
  - Deletion of media

Media Injection Example: RTP

- Real-Time Transfer Protocol
- UDP Transport
- Requisites:
  - Able to observe a legitimate RTP session
- Adjust sequence numbers of injected packets so that they will arrive “before” legitimate packet
- Send away!

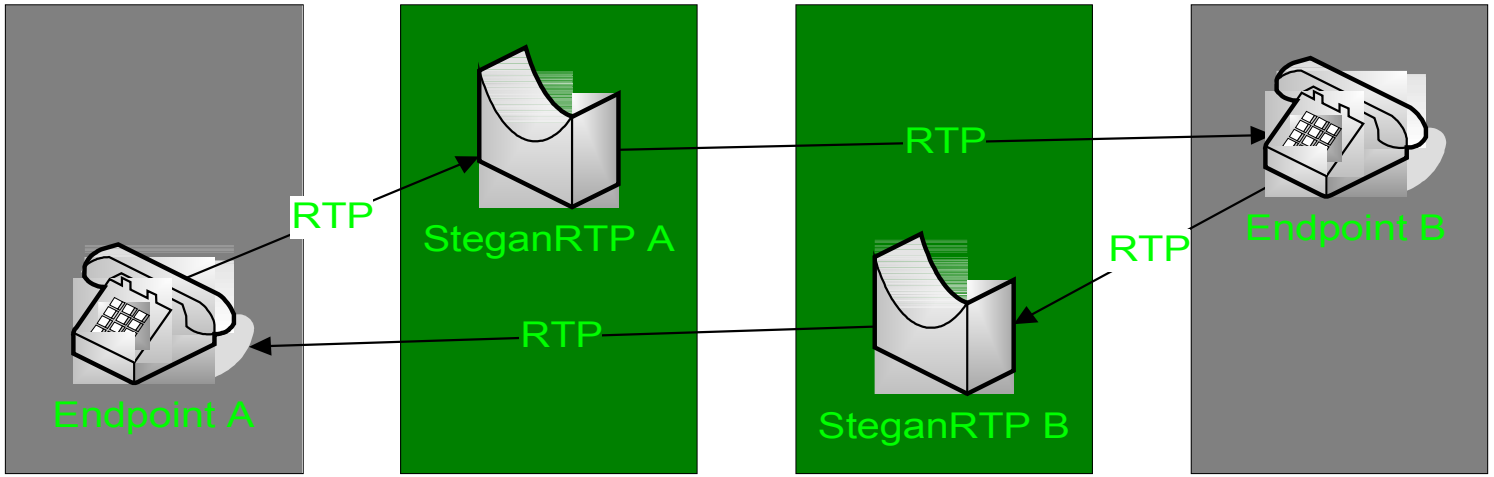
Media Injection

- Tools
  - RTPInsertSound
    - http://www.hackingvoip.com/tools/rtpinsertsound_v3.0.tar.gz
  - RTPMixSound
    - http://www.hackingvoip.com/tools/rtpmixsound_v3.0.tar.gz
  - RTPInject (GUI)
    - http://website.isescpartners.com/files/RTPInject.tar.gz
- Mitigation
  - Authenticate or verify received media packets
  - Encrypt the media channel

Covert Communication

- Vulnerability
  - Media channel packets are unauthenticated and unencrypted
- Attack:
  - Manipulate an active media channel and embed covert communication data
  - Extract covert communication data from an active media channel
- Effect:
  - Send covert data using someone else's call media
  - Receive covert data embedded into someone else's call media

MITM Covert Communication



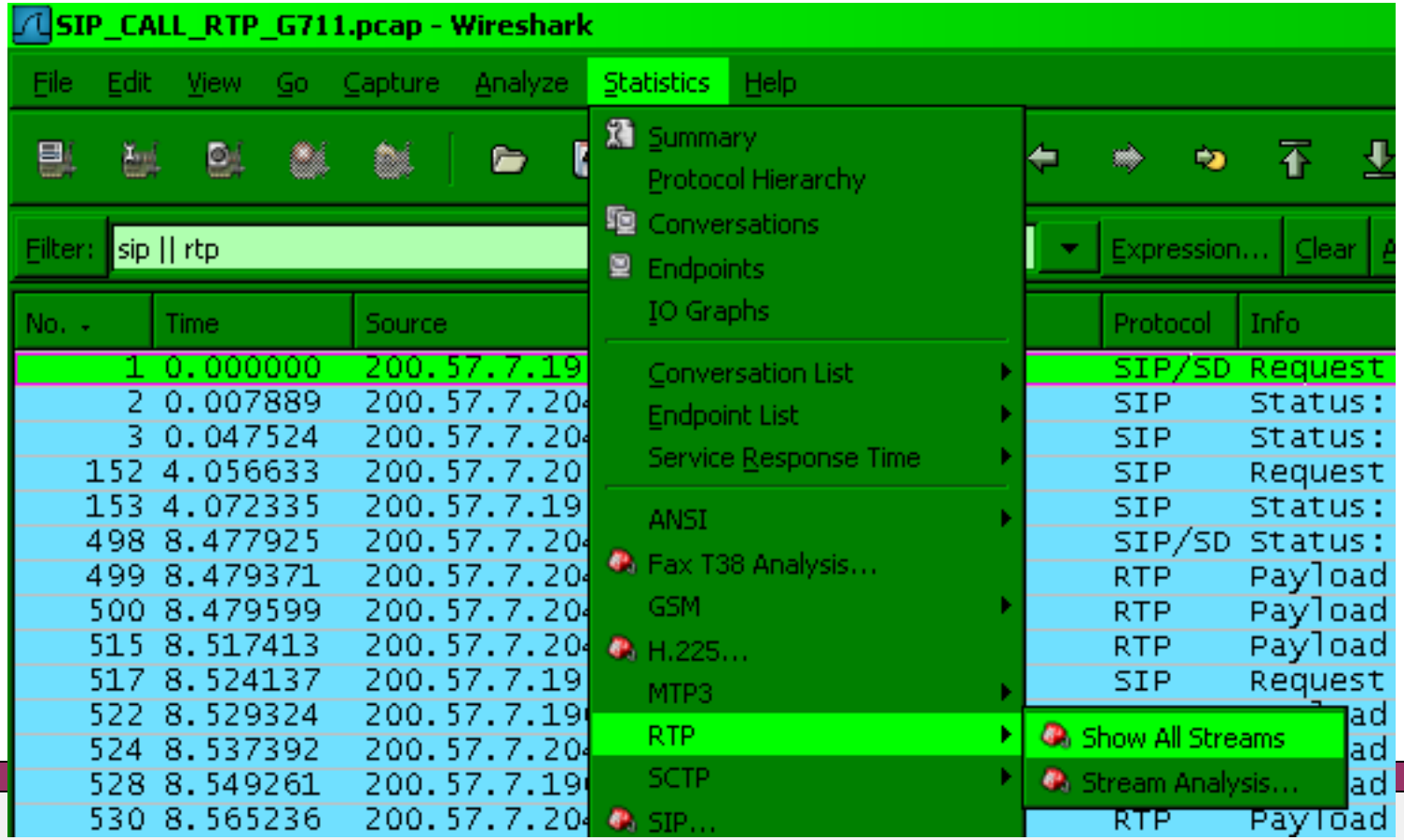
Covert Communication

- Tools
  - SteganRTP
    - http://sourceforgenet/projects/steganrtp/
  - Vo²IP
    - No longer available
- Mitigation
  - Authenticate or verify media packets
  - Encrypt the media channel (some protection)

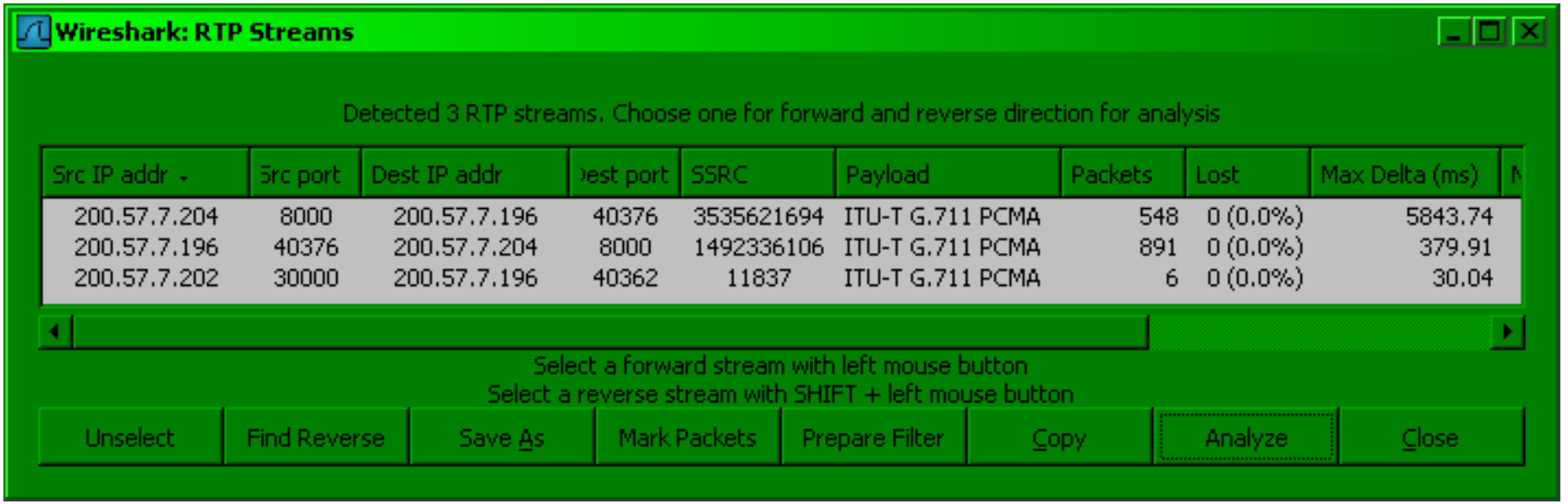
Eavesdropping the Media

- Vulnerability:
  - Media protocols are usually un-encrypted on the wire
  - Media traffic can be observed and recorded
- Attack:
  - Observe / Record the media packets
  - Reconstruct the payload into an easily playable media file
- Effect:
  - Calls are not private!

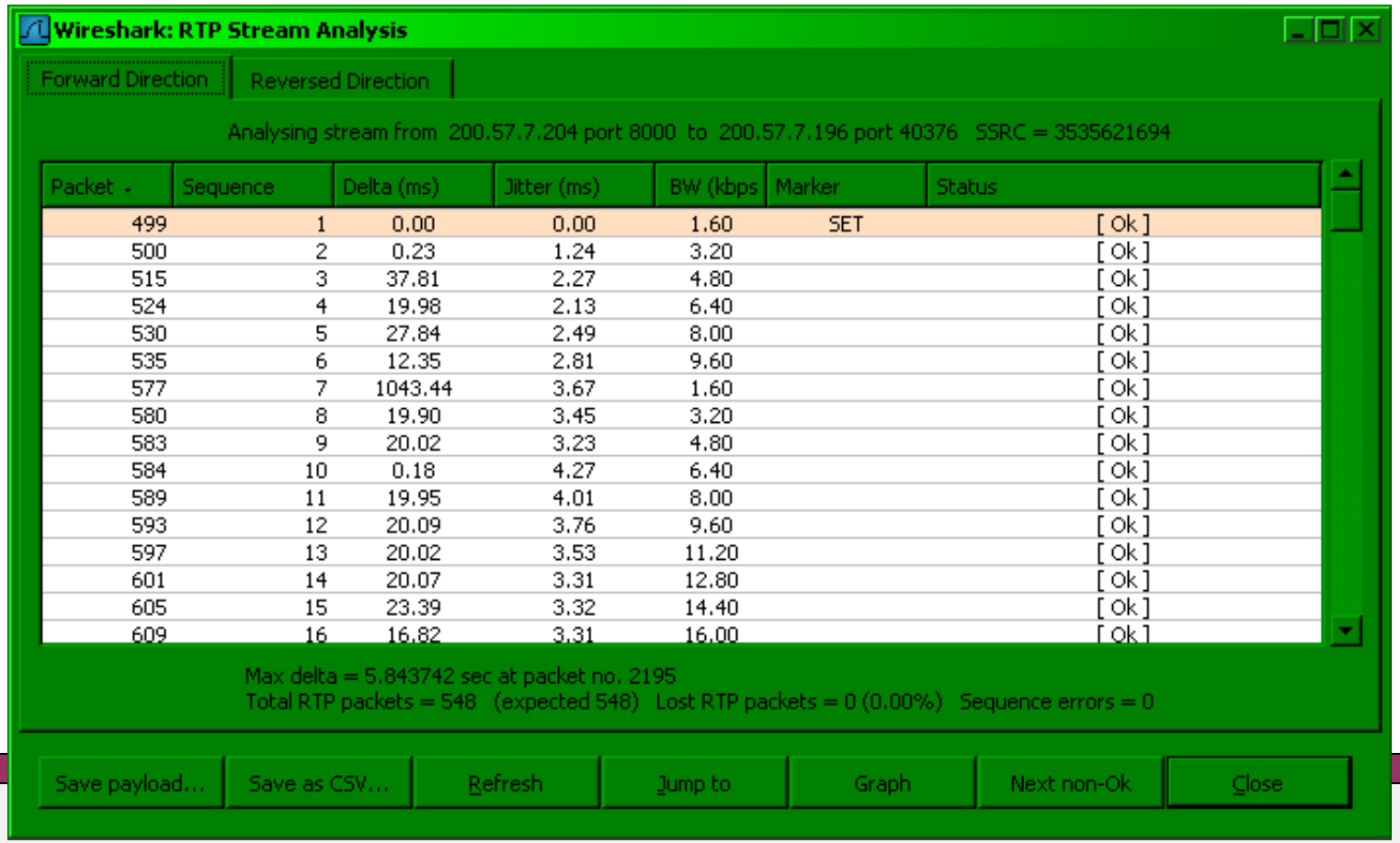
Eavesdropping Example: RTP



RTP Eavesdropping



RTP Eavesdropping



RTP Eavesdropping

Eavesdropping the Media

- Tools:
  - Ethereal / Wireshark
    - http://www.wireshark.org/
  - Cain & Abel
    - http://www.oxid.it/cain.html
  - Vomit - Targets Cisco devices
    - http://vomit.xtdnet.nl/
  - Etherpeek VX
    - http://www.wildpackets.com/products/etherpeek/overview
- Mitigation:
  - Encrypt the media channel

Attacks Leveraging the Underlying Network

Configuration Disclosure: Infrastructure

- Vulnerability:
  - Most hard-phones use FTP or TFTP when booting
  - FTP is an insecure protocol
  - TFTP is an even more insecure protocol
- Attack:
  - FTP: Observe the device's login credentials
  - TFTP: Guess or observe filenames
  - Grab the configuration file and firmware from the server
  - Or just reconstruct the firmware / configuration file from observation
- Effect:
  - Disclosure of sensitive information such as:
    - Usernames / Passwords
    - Call Server, Gateway, Registration Server, etc.
    - Available VoIP services

Configuration Disclosure: Infrastructure

- Tools:
  - Ethereal / Wireshark
    - http://www.wireshark.org/
  - Deductive Reasoning
    - Cisco phones have MAC based filenames:
      - CTLSEP<eth.addr>.tlv
      - SEP<eth.addr>.cnf.xml
      - SIP<eth.addr>.cnf
      - MGC<eth.addr>.cnf
    - Then there's defaults:
      - XMLDefault.cnf.xml
      - SIPDefault.cnf
      - dialplan.xml
  - TFTP-Bruteforce - Brute forces TFTP filenames
    - http://www.hackingexposedcisco.com/tools/TFTP-bruteforce.tar.gz
- Mitigation:
  - Don 't use TFTP! FTP is better, but still not secure...
  - Use non-default filenames

Attacks Against Endpoint Services

Configuration Disclosure: Device

- Vulnerability:
  - Hard-phones provide management interfaces
  - VXWorks remote debugging and console port open
- Attack:
  - Point a browser at the device on port 80
  - SNMP-walk the device
  - Attach a remote VXWorks debugger
- Effect:
  - Disclosure of sensitive information such as:
    - Usernames / Passwords
    - Call Server, Gateway, Registration Server, etc.
    - Available VoIP services
    - Device internals

Configuration Disclosure: Device

- Tools:
  - Web Browser - Connect to port 80
  - SNMPwalk - retrieve a subtree of management values
    - http://net-snmp.sourceforge.net/docs/man/snmpwalk.html
  - VXWorks debugger (GDB)
- Mitigation:
  - Disable device admin ports like HTTP and SNMP
  - Disable remote debugging ports

Web Management Interface XSS

- Vulnerability
  - Devices don't sanitize input / web output
  - Device web management apps display log and message data
- Attack
  - Embed XSS code into a signaling message
  - Send crafted message to target device
  - Wait for user to display logs/message via the device's web interface
- Impact
  - Cross-Site-Scripting code execution
  - Potential traversal of trust boundaries

Web Management Interface XSS

- Tools:
  - Any VoIP device with user-configurable display fields
  - Example:
    - http://voipsa.org/pipermail/voipsec_voipsa.org/2007-October/002452.html
- Mitigation:
  - Don't use device web management interfaces
  - Demand more secure protocol stacks from your device vendors

Vendor-Specific Attacks

Vendor-Specific Attacks

Cisco

Cisco IP Phone Forced Reboot

- Vulnerability:
  - SCCP runs on TCP which is vulnerable to reset attacks
  - If a phone's signaling channel is terminated this way the phone performs a full reboot
  - As of firmware 8.0(7.0) (most recent for 7940, 8.3.3 not avail)
  - Public Disclosure: 04/20/2004
  - http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml
- Attack:
  - Inject a RST packet into the signaling channel
- Effects:
  - The IP phone performs a full reboot
  - Service is unavailable while doing so

Cisco IP Phone: Forced Reboot

- Tools:
  - tcpkill - Sniffs network traffic for a TCP session and injects RST packets to forcibly close the connection
- Vendor Response: 04/20/2004
  - http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml
  - Summary: Fixed adhering to version 2 of http://tools.ietf.org/wg/tcpm/draft-ietf-tcpm-tcpsecure/
  - Result: Attack is slightly harder but not much. Phone still reboots.
- Mitigation:
  - The device should re-establish the session rather than performing a full device reboot.
  - (like when you prompt a RST via an ICMP destination/protocol unreachable (Type 3, Code 2) attack against the CCM (BID:12134))

Vendor-Specific Attacks

FiWin

SS28S Debug Console Hard-coded Credentials

- Vulnerability
  - VxWorks debug console open via Telnet
  - VxWorks credentials hard-coded to user “1” and pass “1”
  - As of firmware 01_02_07 (current as of 10/24/06)
- Public Disclosure: 09/22/06
  - http://www.osnews.com/story.php/15923/Review-FiWin-SS28S-WiFi-VoIP-SIPSkype-Phone/
  - BID: 20154
- Attack
  - Telnet to the phone on port 23
  - Authenticate with username “1”, password “1”
- Effects
  - Device configuration disclosure
  - Authentication credentials disclosure
  - DoS via memory corruption, disk format/corruption

SS28S Debug Console Hard-coded Credentials

- Tools
  - Telnet client
- Vendor Response
  - Notified 09/15/06 by Zachary McGrew, no response.
  - Notified 09/26/06 by myself, no response.
- Mitigation
  - Issue the “td tTelnetd” command within the VXWorks console
  - Update the firmware
    - No updated firmware available
    - Requires proprietary USB cable that you can only get from FiWin
    - They apparently don’t sell it!

Issues With Mitigation

Encrypt the Media Channel

- Many deployed devices don't support SRTP
- Many new devices won't support SRTP yet
- No standard way to negotiate or send keys
- Some methods for keying utilize the unencrypted signaling channel anyway
- ZRTP: DH Key Negotiation within the media channel
- May use IPSec or TLS, but...

Encrypt the Signaling Channel

- There is also no standard way to do this
- Alternatives to encrypting the signaling protocol itself include:
  - IPSec to encrypt at the network layer
    - Not scalable
    - Issues with call set-up times
  - TLS to encrypt at the transport layer
    - Not end-to-end
    - Issues with trust; no global PKI
  - New protocol: DTLS!

Authenticate All Signaling Messages

- Requires that you update/fix the protocols
- The nature of VoIP requires that unknown parties be able to initiate sessions
- Can potentially wrap the protocol in an authenticating transport like IPSec or TLS

Fix the Protocols

- Not an immediate solution
- More time consuming with open / standards based protocols
  - You have to convince a committee there is a problem
  - Deliberation takes time
- May be faster / easier with proprietary protocols
  - But you have to convince the vendor there is a problem

Don't Trust Caller-ID

- Unfortunately, users have been trained to believe that Caller-ID is trustworthy
- Caller-ID *should* be trustworthy
- Will take time to educate users

Use open-source soft-phones / firmware

- Unfortunately, most open-source soft-phones also have poor protocol stacks
  - But at least you can:
    - Audit the code
    - Report problems to the maintainers
- As far as I'm aware, there is no open source firmware for hard-phones
  - Most are vendor-proprietary

Demand Resilient Vendor Devices

- Vendors aren't motivated to improve device security
- Some devices in this area are getting better
- Phones are limited by their hardware

Rate-limit Offensive Traffic

- Low-rate floods still effective! (just differently)
- Low-rate floods look like legitimate traffic
- Media doesn't like latency

Don't use TFTP! (or FTP)

- Most vendor VoIP systems don’t provide an alternative

Conclusions

Q&A