VoIP Attacks!

Dustin D. Trammell
VoIP Security Research
TippingPoint, a division of 3Com
Computer Academic Underground

About Me

- I)ruid / Dustin D. Trammell
- Employed by TippingPoint, a division of 3Com
  - http://www.tippingpoint.com/security/
- Founder, Computer Academic Underground
  - http://www.caughq.org/
- Instigator, AHA! (Austin Hackers Anonymous)
  - http://www.austinhackers.org/
- Contributor, VoIP Security Alliance projects/blog
  - http://www.voipsa.com/

About this Presentation

- All attacks discussed are either recently developed, or extremely significant
- Making the case that attack tools are both 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; not social attacks like SPIT, Phishing, etc.
- Tim Burton is AWESOME!

Notes on Mitigation

- Many times there are no clear-cut "solutions" to any vulnerability or attack
- I will refrain from using the "so just isolate your VoIP network" cop-out "solution"
- Some mitigation techniques suggested 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

C.M.A.

- All *Mars Attacks!* Audio and Video is Copyright Warner Brothers Pictures (Time Warner Entertainment)

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!

Attacks Against Availability

Flooding

Flooding

- Vulnerabilities:
  - Most hard-phones are 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
    - UDP
- 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

Fuzzing

- Vulnerabilities:
  - Protocol stack implementations suck
- Attack:
  - Send malformed messages to a device’s input vectors
- Effect:
  - Most endpoint devices will crash, halt, freeze, or otherwise respond poorly
  - Some core devices may behave similarly
  - You may find bugs that do more than just provide a Denial of Service

Fuzzing

- Tools:
  - 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

Forced Call Teardown

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
    - SCCP: Reset (Message type 159 (0x9f))
    - 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 messages such as BYE into an existing session
    - http://skora.net/uploads/media/sip-kill
  - sip-proxykill - Similar technique against SIP proxies
    - http://skora.net/uploads/media/sip-proxykill
- Mitigation:
  - Encrypt the signaling channel
  - Authenticate every signaling message

Registration/Call Hijacking

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

Registration Hijacking

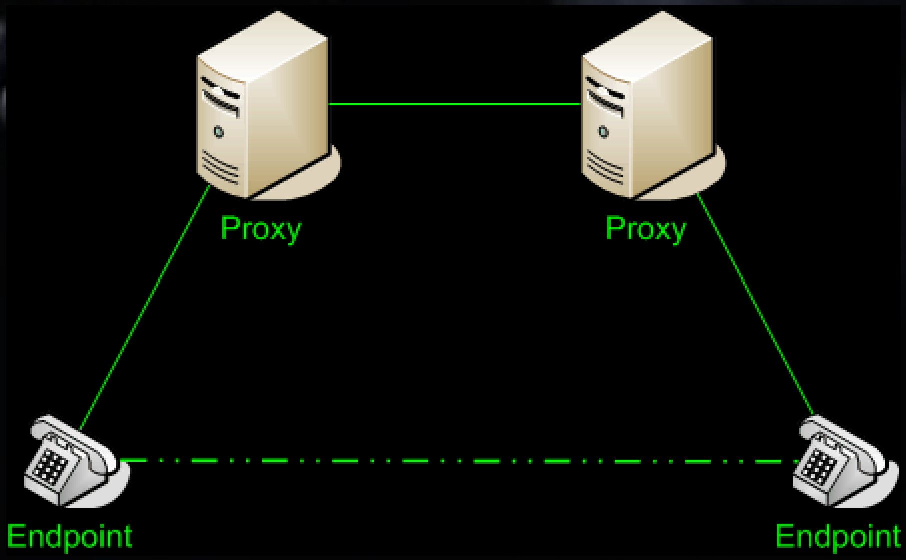
- Tools
  - Registration Hijacker
    - http://www.hackingexposedvoip.com/tools/reghijacker.tar.gz
  - Registration Remover
    - http://www.hackingexposedvoip.com/tools/eraseregistrations.tar.gz
  - Registration Adder
    - http://www.hackingexposedvoip.com/tools/add_registrations.tar.gz
  - RedirectPoison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

Attacks Against Integrity

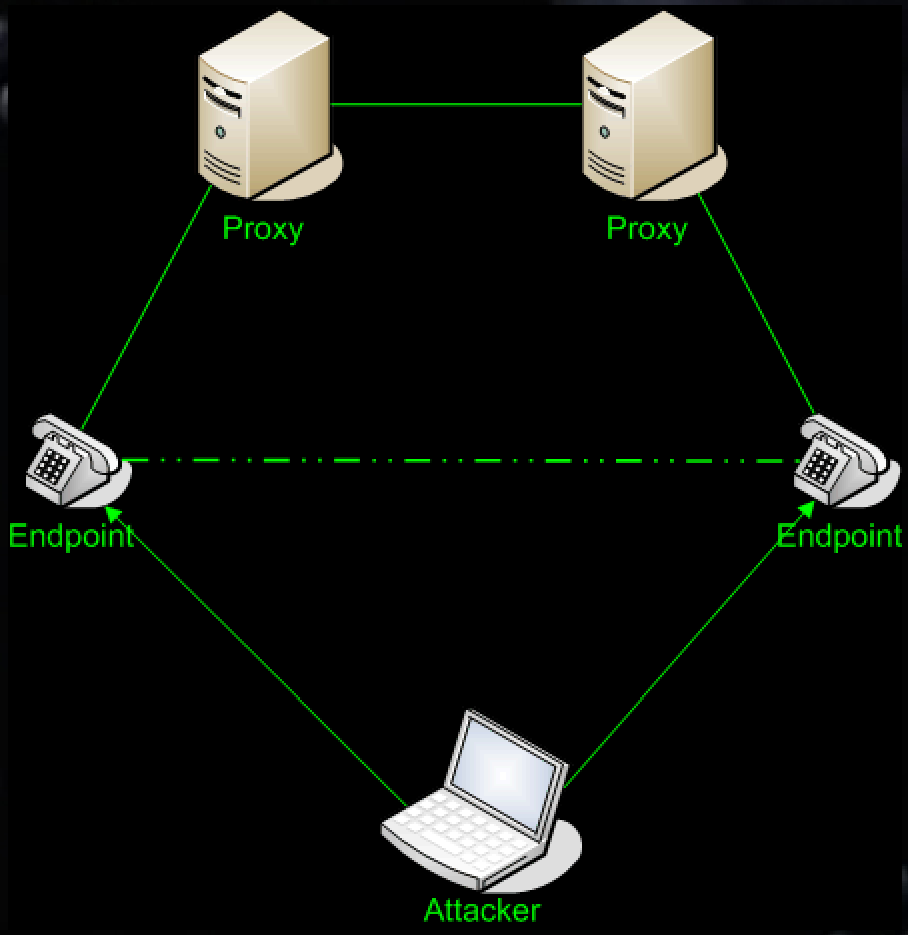
Media Hijacking

- 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

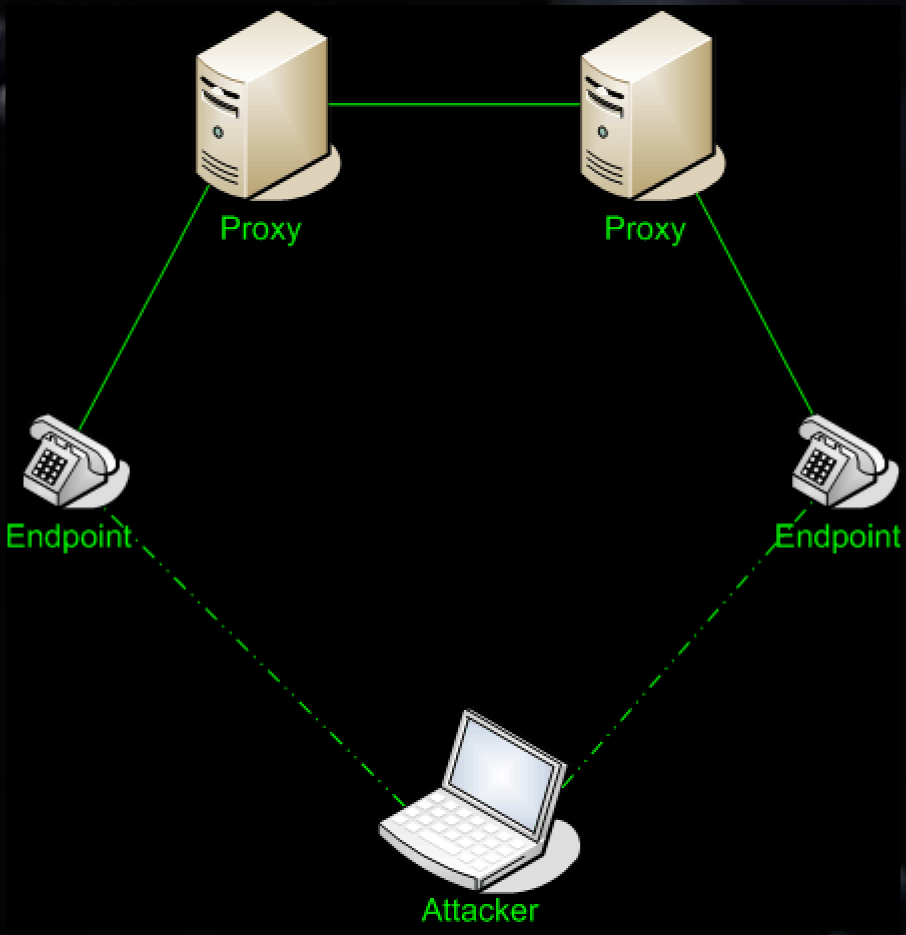
Media Hijacking Example



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

Media Injection

Media Injection

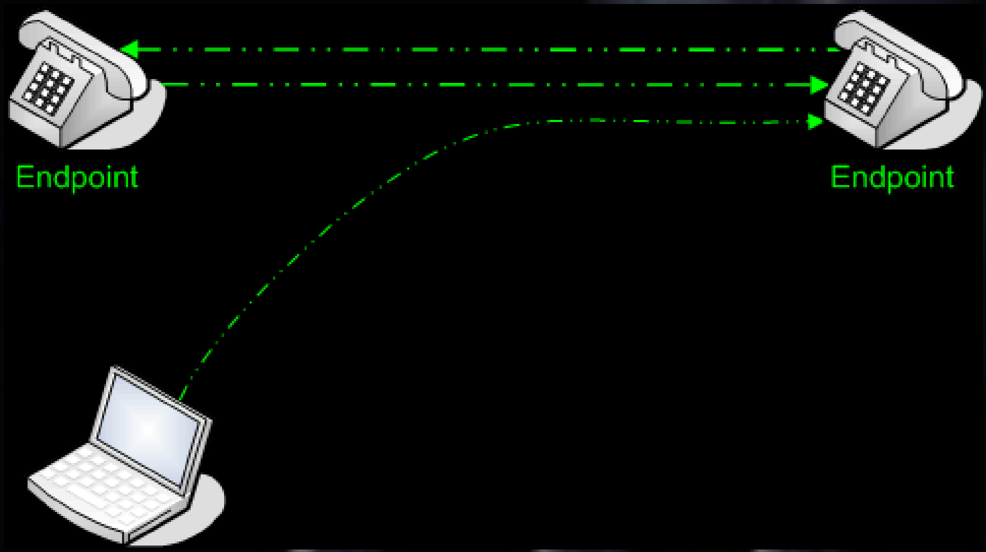
- Vulnerability
  - Media channel packets are unauthenticated and unencrypted
- Attack:
  - Inject new media into an active media channel
  - Replace media in an active media channel
- Effect:
  - Modification of media
  - Replacement of media
  - Deletion of media

Media Injection Example: RTP

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

RTP Injection

RTP Injection



- IPID = IPID + spoof-factor
- sequence = sequence + spoof-factor
- timestamp = timestamp + (payload-len * spoof-factor)

Demo!

RTP Audio Injection

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
- Mitigation
  - Authenticate or verify media packets
  - Encrypt the media channel

Caller-ID Spoofing

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 VoIP 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

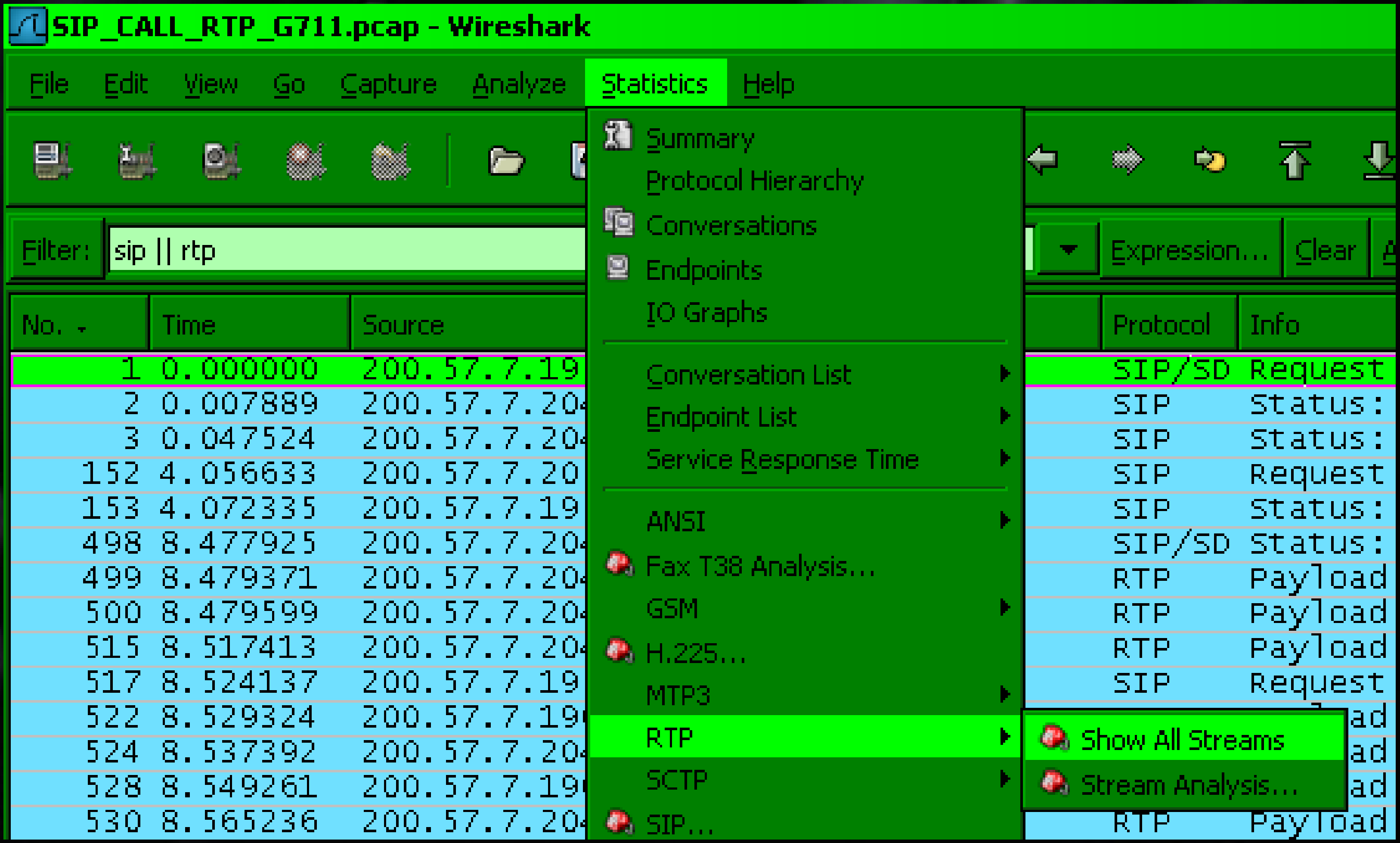

Attacks Against
Confidentiality

Eavesdropping the Media

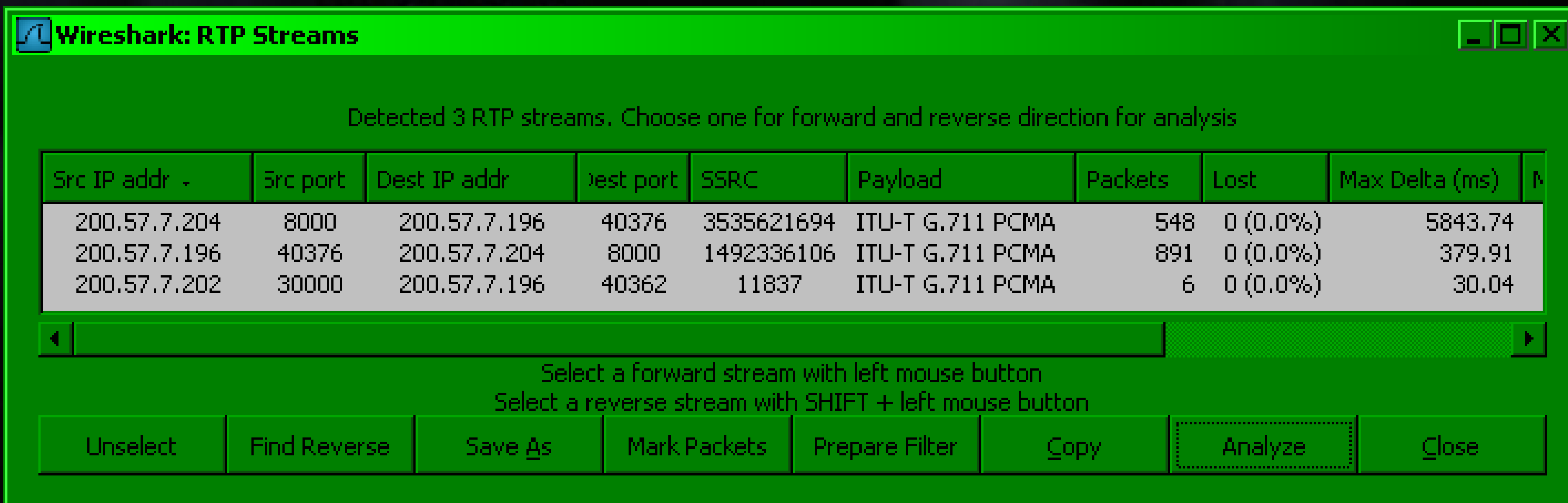
Eavesdropping the Media

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

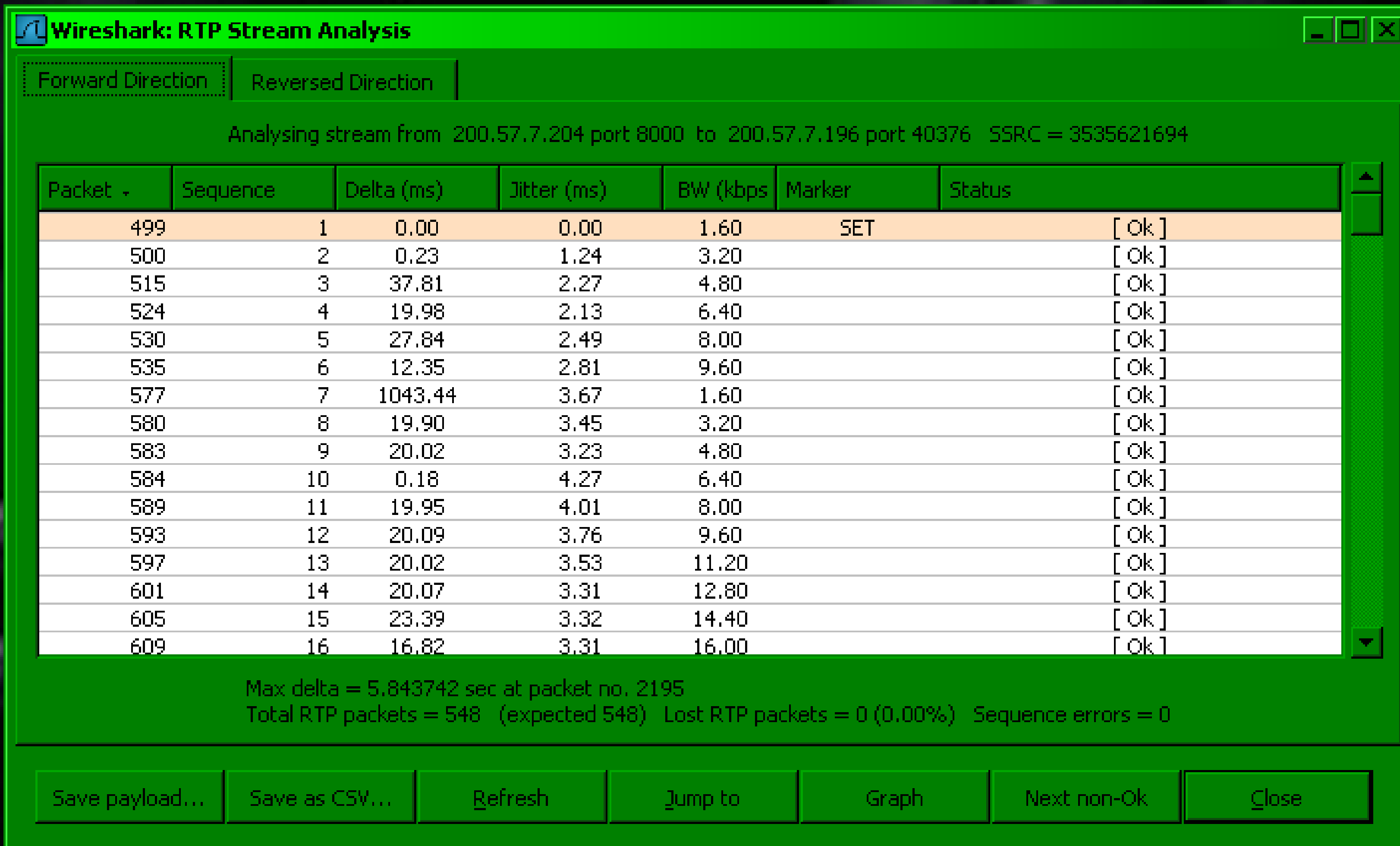
Eavesdropping Example



Eavesdropping Example



Eavesdropping Example



Wireshark: RTP Stream Analysis

Forward Direction | Reversed Direction

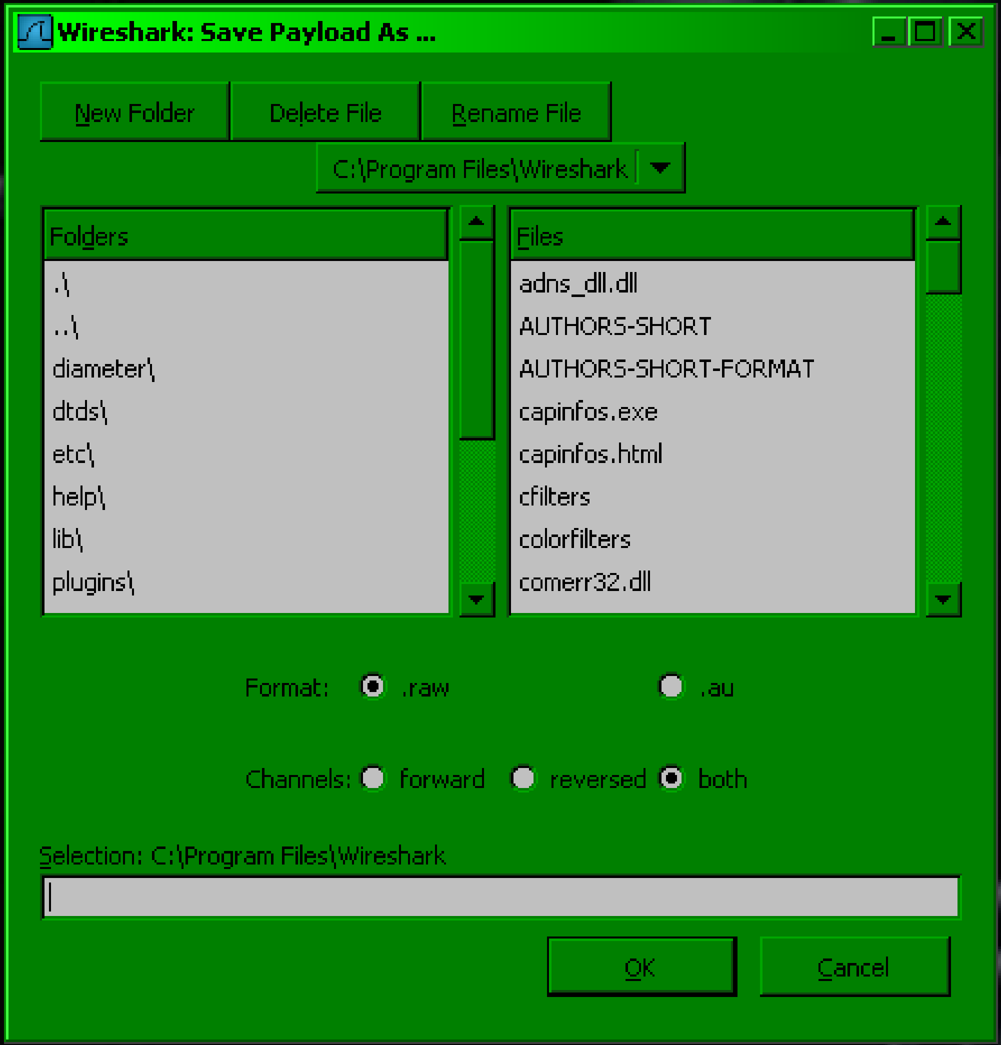
Analysing stream from 200.57.7.204 port 8000 to 200.57.7.196 port 40376 SSRC = 3535621694

Packet	Sequence	Delta (ms)	Jitter (ms)	BW (kbps	Marker	Status
499	1	0.00	0.00	1.60	SET	[Ok]
500	2	0.23	1.24	3.20		[Ok]
515	3	37.81	2.27	4.80		[Ok]
524	4	19.98	2.13	6.40		[Ok]
530	5	27.84	2.49	8.00		[Ok]
535	6	12.35	2.81	9.60		[Ok]
577	7	1043.44	3.67	1.60		[Ok]
580	8	19.90	3.45	3.20		[Ok]
583	9	20.02	3.23	4.80		[Ok]
584	10	0.18	4.27	6.40		[Ok]
589	11	19.95	4.01	8.00		[Ok]
593	12	20.09	3.76	9.60		[Ok]
597	13	20.02	3.53	11.20		[Ok]
601	14	20.07	3.31	12.80		[Ok]
605	15	23.39	3.32	14.40		[Ok]
609	16	16.82	3.31	16.00		[Ok]

Max delta = 5.843742 sec at packet no. 2195
Total RTP packets = 548 (expected 548) Lost RTP packets = 0 (0.00%) Sequence errors = 0

Save payload... | Save as CSV... | Refresh | Jump to | Graph | Next non-Ok | Close

Eavesdropping Example



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

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 and 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.

Configuration Disclosure: Infrastructure

- Vulnerability:
  - Most hard-phones use FTP or TFTP when booting
  - TFTP is an insecure protocol
  - FTP is an insecure protocol
- Attack:
  - FTP: Sniff the device's login credentials
  - TFTP: Guess or sniff the filenames
  - Grab the configuration file and firmware from the server
  - Or just sniff the firmware and configuration file from the wire
- 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

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
  - GDB configured for VXWorks support
- Mitigation:
  - Disable device admin ports like HTTP and SNMP
  - Disable remote debugging ports

Mitigation

Encrypt the Media Channel

- Not many devices support SRTP yet
- No standard way to negotiate or send keys
- Keys are generally negotiated or sent in the unencrypted signaling channel anyway
- ZRTP: DH Key Negotiation within the media channel, doesn’t comply with CALEA
- May use IPSec or TLS, but...

Encrypt the Signaling Channel

- There is 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

Authenticate All Signaling Messages

- Requires that you update/fix the protocol
- 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

Demand resilient devices from your VoIP device vendor

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

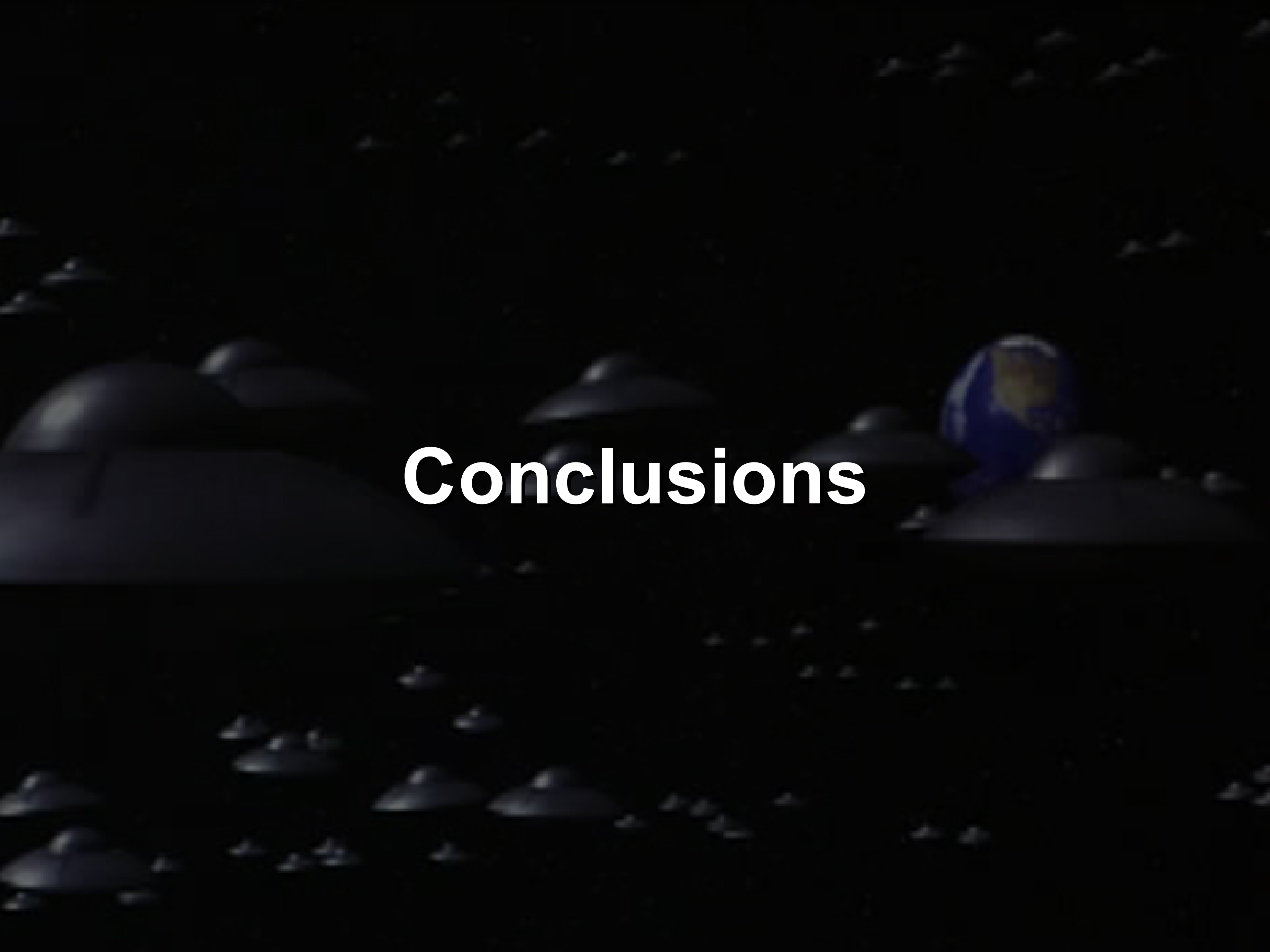
Rate-limit Offensive Traffic

- 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 architectures don’t provide an alternative

Conclusions



Q&A

Fin.