

# To V☺IP or not to V☹IP... ...esa es la cuestión

  
www.raulsiles.com

VII Foro de seguridad RedIRIS  
Arquitecturas Seguras



RedIRIS

12 de marzo de 2009



© 2009 Raúl Siles. Todos los derechos reservados.

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

## Index

- Data & Voice communications
- Traditional telephony vs. VoIP
- VoIP 101
- (A few) VoIP Attacks
- VoIP Defenses
- Summary



VoIP, Hollywood & Real-Life



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

2

## Until Now..., It's ALL about Data

- Firewalls, NIDS/IPS, HIDS/IPS, AV, Anti-spyware/malware, log and patch management, web application FW, etc
- Network devices and host hardening, intrusion detection, incident handling, perimeter protection, forensics, database security, wireless security, etc
- Data confidentiality, integrity & availability
- Defense-in-depth
  - Secure architectures

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

3

## Voice Communications...

- What is your preferred communication method?
- Are you using VoIP? Are you sure????
- VoIP is here to stay!!
- Service providers, carriers, and enterprises (and personal communications - FTTH)
- Weaknesses and vulnerabilities on the original design, protocols and specs

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

4

## Traditional Telephony vs. VoIP



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

5

## Traditional Telephony

- PSTN (or POTS)
- Cellular networks
  - GSM, GPRS, or UMTS
- Analog or digital communications
- Closed and proprietary nature
- Signaling based on ISDN, SS7, or SS7/MAP (GSM)

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

6

## Traditional Telephony (2)

- Expectation of privacy and level of trust in the legacy telephony infrastructures
- PSTN: Physical security
  - Neighborhood or end-to-end path
- GSM: Radio waves (bands)
  - MitM attacks (impersonate Base Station)
  - THC-GSM project/sniffer (GNU radio)
    - A5/1 & A5/2 encryption (FPGAs)

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

7

## Voice Signaling Attacks

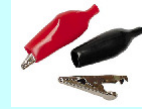
- In-band frequency signaling
- Phreaking culture, 1971
- 2600 Hz tones
- E.g. Captain (Cap'n) Crunch, Steve Wozniak, Steve Jobs...
- Network segmentation: ISDN and SS7



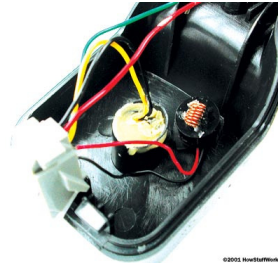
To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

8

## Voice Media Attacks



- Analog hidden-phone, alligator clips, tape recorder, or bug
- Modern PSTN or cellular nets
  - Digital switches
- E.g. Greek wiretapping ring (2004-05)
- Phone encryption
  - PSTN, GSM
- Wiretap detectors



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

9

## VoIP

- Voice over IP
- Main VoIP concerns:
  - Lowering the telecommunication costs
  - Cost reduction, computer application integration, and unified communications
  - Security
- Open and distributed nature of VoIP infrastructures
- Inherit the IP-based security threats



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

10

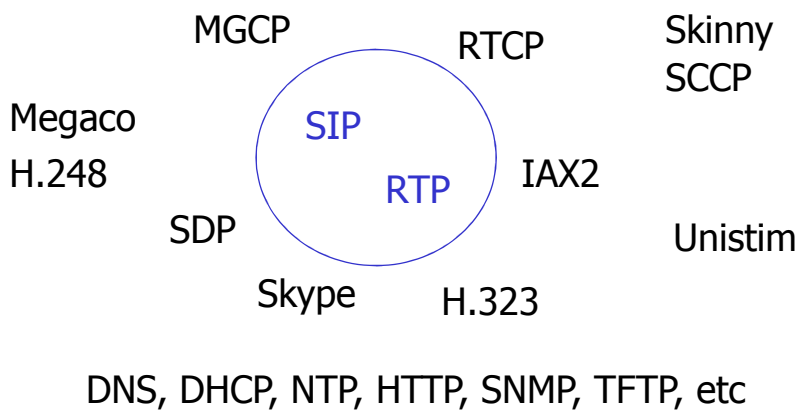
## VoIP vs. Data

- Joining two (different) worlds together
- It's all about IP!!
- Real-time nature of VoIP communications
- Network convergence
- New VoIP protocols
- New VoIP application-layer security devices

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

11

## VoIP Protocols



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

12

## Are we improving security for VoIP while reducing security for the rest of the network?

- Does the improved security just apply to telephony itself?
- VoIP protocols were designed to be hardly secured 😊
- VoIP makes more difficult to protect the whole IP network
- *Devil's advocate* 😊

<http://radajo.blogspot.com/2007/10/are-we-improving-security-for-voip.html>

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

13

## Are we improving security...?

- Security vs. Complexity
- Security-friendly protocols?
  - H.323 vs. SIP vs. IAX2
- Conventional firewalls:
  - Similar to HTTP/Web Services/Web 2.0
- Network segregation (layer 2/3/4...) to mitigate unified communications risks

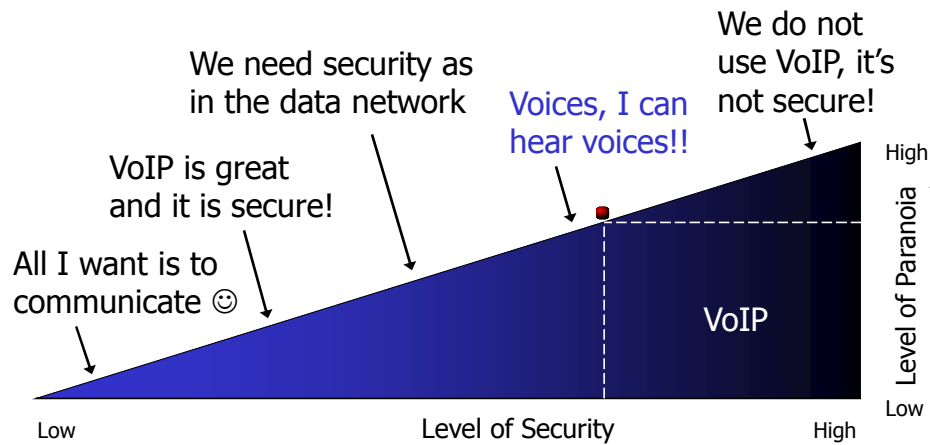


Redesign (& secure) your network architecture

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

14

## VoIP Paranoid-meter



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

15

## VoIP Security Threats

- Receive someone's calls (C, I)
- Make calls impersonating someone (I)
  - Spoofing
- Capture conversations (C)
  - Eavesdropping
- Modify conversations (C, I, A)
  - MitM
- Denial of service, DoS (A)



VoIP infrastructure, signaling, and media threats

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

16



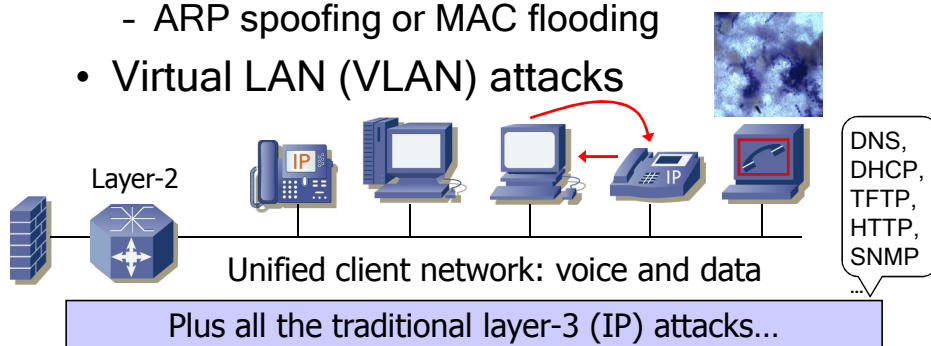
## (A few) VoIP Attacks

- Layer-2 attacks & VoIP hopping
- Google hacking - VoIP
- PBX fingerprinting
- Wardialing (using VoIP)
- Caller ID spoofing
- Eavesdropping VoIP: signaling & media
- VoIP media manipulation
- Vishing & Real-world attacks



## Layer-2 Attacks

- Unified communications (single net)
- Sniffing, interception & redirection
  - ARP spoofing or MAC flooding
- Virtual LAN (VLAN) attacks



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

18

# VoIP Hopping Attack

- VoIP hardphone (acts like a switch)
  - Single Ethernet cable (voice & data)
- Get physical access to the phone & sniff traffic
  - Meeting rooms, reception, etc
- Enable attacker's computer in "Voice VLAN" ID
- The computer belongs to the VoIP VLAN and can... attack! (trunk port)



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

19

# VoIP Hopping Attack (2)

- Manually: vconfig & ARP spoofing
- Voiphopper (listen CDP & reconfigure NIC)
- ACE: Automated Corporate Enumerator
  - Get corporate directory as a Cisco IP phone

```
Starting Unified sniffing...
Listening for new calls to or from target John (CEO) Rodgers (Extension 1004, IP 172.16.96.18)
Endpoint station Caller ID 1090 calling target
Target John (CEO) Rodgers (Extension 1004, IP 172.16.96.18) went offhook
Endpoint station Caller ID 1090 calling target
Target call in progress at 16:56:8, receiving call from 1090
Starting media capture between target and Eric Winsborrow (Extension 1004)
Endpoint station Caller ID 1090 calling target
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)
```

UCSniff - Unified Communication Sniffer

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

20

# Google Hacking - VoIP

- Why?
  - Google hacking → Web → VoIP
- GHDB:
  - Book - Volume II (pg. 446)
  - VoIP:
    - Various Online Devices
    - Pages containing login portals

<http://johnny.ihackstuff.com/ghdb.php>  
<http://www.hackingvoip.com/google.html>

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

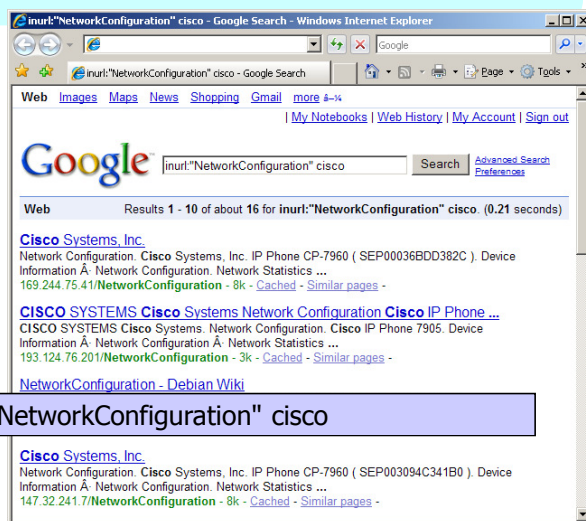
21

# Google Hacking - VoIP (2)

Cisco  
hardphones:  
(CP-7960)



`inurl:"NetworkConfiguration" cisco`



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

22

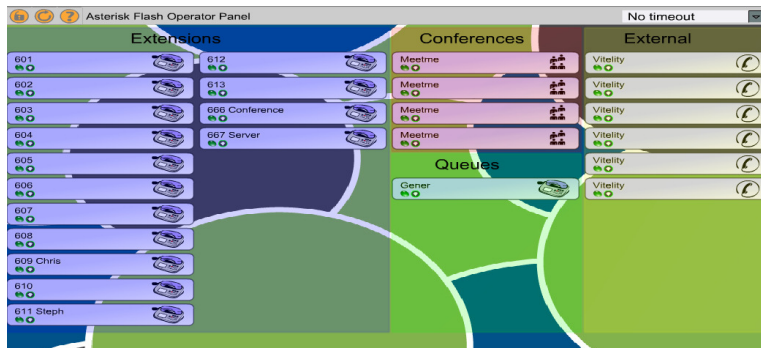
## Google Hacking - VoIP (3)

The screenshot shows a Cisco IP Phone configuration page. The left sidebar contains navigation links such as 'Device Information', 'Network Configuration', 'Network Statistics', 'Ethernet', 'Port 1 (Network)', 'Port 2 (Access)', 'Port 3 (Phone)', 'Device Logs', 'Debug Display', 'Stack Statistics', 'Status Messages', 'Streaming Statistics', 'Stream 1', and 'Stream 2'. The main content area is divided into two sections: 'Device Information' and 'Network Configuration'. The 'Device Information' section lists details for a Cisco Systems, Inc. IP Phone CP-7960 (SEP00036BDD382C), including MAC Address, Host Name, Phone DN, App Load ID, Boot Load ID, Version, DSP, Expansion Module 1, Expansion Module 2, Hardware Revision, Serial Number, Model Number, Codec, Amps, C3PO Revision, and Message Waiting. The 'Network Configuration' section lists DHCP Server, BOOTP Server, MAC Address, Host Name, Domain Name, IP Address, Subnet Mask, TFTP Server, and Default Router 1 through 4. A red arrow points from the 'IP Address' field in the 'Device Information' section to the 'IP Address' field in the 'Network Configuration' section. Another red arrow points from the 'DNS Server 1' field in the 'Network Configuration' section to the 'DNS Server 1' field in the 'Network Configuration' section. A third red arrow points from the 'Information URL' field in the 'Network Configuration' section to the 'Information URL' field in the 'Network Configuration' section. A fourth red arrow points from the 'Services URL' field in the 'Network Configuration' section to the 'Services URL' field in the 'Network Configuration' section.

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles 23


## Google Hacking - VoIP (4)

- Flash Operator Panel: switchboard Asterisk PBX
  - <http://johnny.ihackstuff.com/ghdb.php?function=detail&id=1134>



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles 24

## PBX fingerprinting

- Manual PBX identification
- Collection of default sound files of popular VoIP voicemail systems to assist in properly identifying the vendor
  - Asterisk, Avaya, Cisco... 
  - Risk of default settings!!
- Change ALL settings: tech and human

<http://www.hackingvoip.com/voicemail.html>

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

25

## Wardialing (using VoIP)

- Wardialing on steroids (without a modem)
- xDSL (home) + VoIP provider account
  - 1000 phone lines or numbers / hour
- Record audio (archived) & signatures
  - Modems, faxes, voice mailbox, PBX, loops, dial tones, IVR, forwarders, etc (classify)
- Like nmap for the PSTN
- Laws regulating automated dialing

WarBOX

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

26

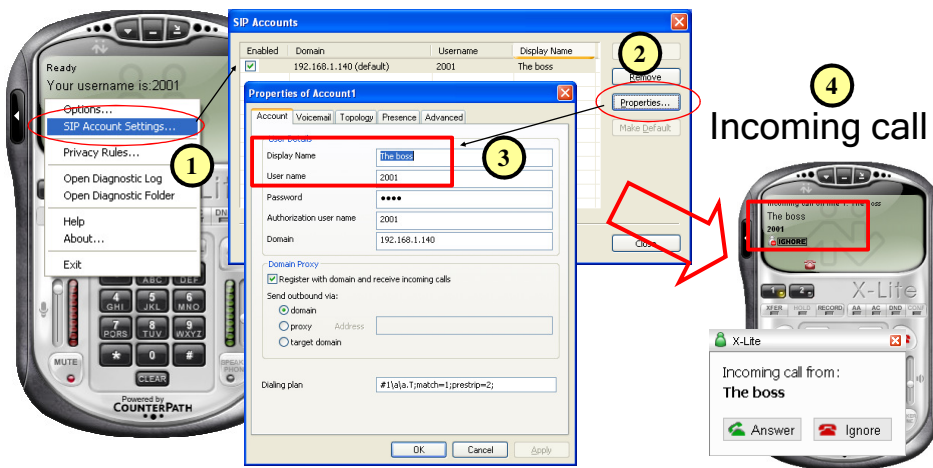
## Caller ID spoofing

- Common “trusted” authentication mechanism
  - Relative, boss, bank, etc
- Trivial and unavoidable in the PSTN
- Strong authentication methods are available in VoIP
  - + Anti-SPIT (RFC 5039)
- Mitigate impersonation attacks

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

27

## Caller ID Spoofing (2)



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

28

# Caller ID Spoofing (3)

**Spoofed INVITE**

**Spoofed caller ID**

**Attacker**

**Valid SDP contents**

To VoIP or not to

# Caller ID Spoofing Services

- Spoof the caller ID on all your phone calls (VoIP or PSTN)
- Pay per call/minute services: Spoofcard, Telespoof, SpoofTel...
- Some VoIP providers use similar techniques for some of their offering: Web-based user to user calls

**NEW! Make a FREE trial call!**

Your phone number:

Destination phone number:

Enter both phone numbers in the international format, for instance: 00442012345678.  
Free calls are limited and only valid for landlines in destinations marked as free.  
More instructions.

... "intended for entertainment purposes only"

# Eavesdropping VoIP Call Signaling

Wireshark: "Statistics" → "VoIP Calls"

The screenshot shows the Wireshark interface with the 'Statistics' pane expanded to 'VoIP Calls'. A table lists detected calls with columns for Start Time, Stop Time, Initial Speaker, From, To, Protocol, Packets, State, and Comments. The selected call is highlighted in blue.

Start Time	Stop Time	Initial Speaker	From	To	Protocol	Packets	State	Comments
508.34	575.43	192.168.1.2	sip:816666@voip.brurjula.net	sip:97239287044@voip.brurjula.net	SIP	18	CANCELLED	
692.95	727.34	192.168.1.2	sip:voi18062@sip.cybercity.dk	sip:0097239287044@sip.cybercity.dk	SIP	8	REJECTED	
1307.68	1359.22	192.168.1.2	sip:35104723@sip.cybercity.dk	sip:0097239287044@sip.cybercity.dk	SIP	7	REJECTED	
1425.60	1443.51	192.168.1.2	sip:35104723@sip.cybercity.dk	sip:35104724@sip.cybercity.dk	SIP	8	REJECTED	

Buttons for 'Graph' and 'Player' are highlighted with red boxes.

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

# Eavesdropping VoIP Media (RTP)

Statistics → "VoIP Calls" → Player

The screenshot shows the 'Wireshark: RTP Player' window. A green waveform represents the dial tone. A callout box points to the beginning of the waveform with the text 'Dial tone (two secs.)'. The 'Decode' button is highlighted with a red box.

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles



# Eavesdropping VoIP Signaling, Media, Authentication...

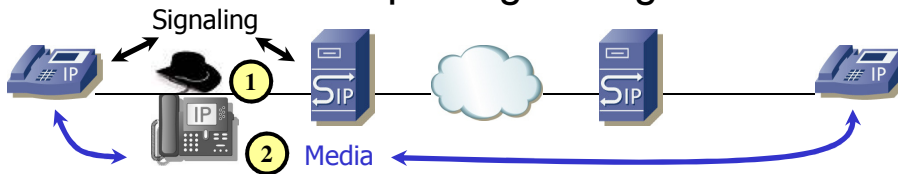
Cain & Abel → "Sniffer" → "VoIP" ①

The screenshot shows the 'Sniffer' tab in Cain & Abel. A table lists captured packets with columns for Started, Closed, IP1 (Codec), IP2 (Codec), Status, File, and Size. A context menu is open over a file, showing options: Play, Remove, Delete, and Remove All. The 'Play' option is highlighted with a red box. Below the screenshot, the text 'Windows Media Player (.wav files) ③' is present, with an arrow pointing to the 'Play' option. A yellow circle with the number '2' is also present near the context menu.

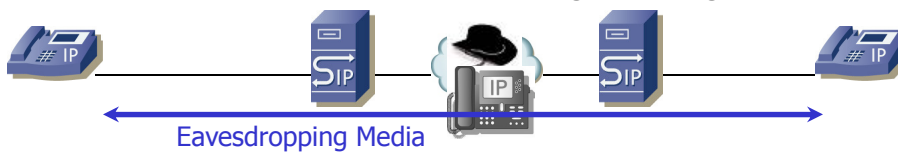
To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles 33

# VoIP Media Manipulation

- MitM attack: Replacing/Mixing audio

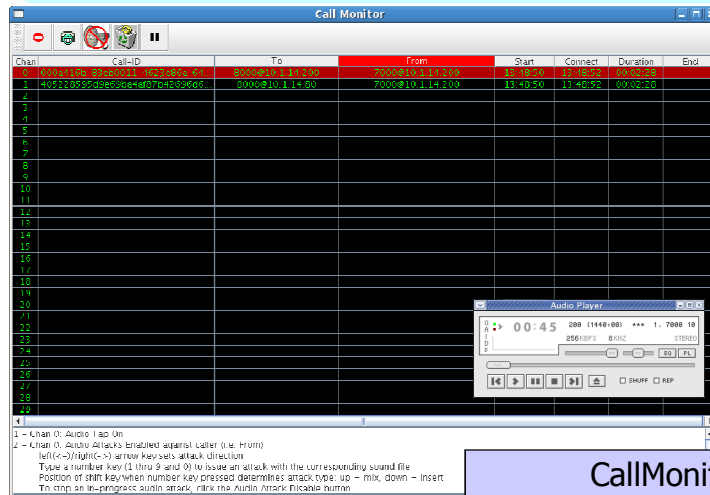


- Non-MitM attack: Inserting/Mixing audio



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles 34

## VoIP Media Manipulation (2)



- Monitor, tear down, tap & insert audio

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

35

## Vishing - Voice Phishing

- Someone calling you impersonating the bank
- Important message (e-mail) asking user to call a specific phone number
- Inherent trust in phone numbers
  - Caller ID spoofing ☺
- System ready to gather sensitive information (CC#, expiration date, PIN#, etc)



<http://isc.sans.org/diary.html?storyid=3486 & 4946>

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

36


## Vishing - Real Incidents

- Enhancements over time
  - Record voice snippets of the target IVR (Interactive Voice Recording) system
- Easily accomplished through Asterisk and recorded audio files
  - Similar to duplicate a Web site in a traditional Phishing scam (except SSL)

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

37

## Vishing - Real Incidents (2)

- Federal Trade Commission (FTC) 
  - IR: Warn customers that the phone number they called is being used to scam personal information
- Call forwarding through VoIP ISP accounts (like Vonage)
  - Compromised through Web page (login credentials)
  - Others: Asterisk, traditional PBX...

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

38

## Vishing - Real Incidents (3)

- More control checks on expected information (e.g. data length, expiration date format...)
- Text-to-voice systems, so they can change the message and not leave a voice print behind (forensic evidence)
- SMS-attacks using a VoIP infrastructure
  - "Your bank account has been locked due to a possible compromise. Please call 800... to re-activate your account." (related Trixbox scanner)

<http://isc.sans.org/diary.html?storyid=4507>

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

39

## Vishing Best Practices

- Verify the number belongs to the "calling" company
  - Company Web page or printed material
  - Unfortunately, we're used to search engines
- Directly call the company number instead of trusting a received caller ID
  - Did I mention you cannot trust the caller ID?
- Counterhack: Reverse Vishing & SEO

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

40

## Reverse Vishing and SEO

- Use search engine optimization (SEO) poisoning techniques
  - Fake phone numbers associated to legitimate organizations on top of the list
- Encourage the victim to call the fake number
- My prediction for the near future...
  - Compromise the company Web page to subtly modify the numbering data

<http://isc.sans.org/diary.html?storyid=4996>

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

41

## Phone Number Authentication

- Add strong authentication to ENUM (E.164 numbers - domain names) & DNS
- Correlate phone numbers from  $\neq$  sources:
  - Company Web page, printed material, multiple search engines, and specific phone queries
  - Specific phone searching services: Who Called Us, 800Notes, NumberZoom, Switchboard.com, Whitepages.com, Reversephonedirectory.com, or Phonenumber.com (US-centric)

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

42

## Bogus Robocall Tells Floridians They Can Vote By Phone

- US elections (October 31, 2008)
- Residents of Broward County, Florida
  - Vote by phone on Election Day
  - The voice identifies herself as Elections Supervisor Brenda Snipes
  - Voting by phone is not allowed
- Residents of the Pittsburgh region
  - Votes on two different dates (Republicans/Democrats)
- Can you say...VoIP!!

<http://blog.wired.com/27bstroke6/2008/10/bogus-robocall.html>

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

43

## Trixbox Scans in 2009

- Scanning for Trixbox vulnerabilities
  - February 2009 (SMS-scams before that...)
- HTTP scans now include...
  - Cisco Domit RSS feature
- Discovery of 0-day: disclose the contents of local files through the Web server (pass hash)

```
xxx.xxx.xxx.xxx - - [31/Jan/2009:00:58:15 -1000] "GET /cisco/services/rss/DOMIT/domit_rss/domitBanner.gif HTTP/1.1" 404 26 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows 98)"
```

<http://isc.sans.org/diary.html?storyid=5782>

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

44

## VoIP Defenses

- Secure network architectures (by design)
- Layer-2 robust architectures
- VoIP network traffic segregation
  - The VoIP softphone paradox
- Secure VoIP protocols
- VoIP security devices
- Integrating VoIP into security



## Secure Network Architectures (by design)

- Defense in depth and layered security principles
- Physical network segregation?
- Logical segregation using VLAN's
  - Define multiple VLAN's: voice, data, management, backup, etc.
- Apply strong layer-3 controls and traffic filters between VLAN's (voice & data)
- VoIP hardphones in the office and VoIP softphones only for road warriors

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

46

## Layer-2 Robust Architectures

- Layer-2 security
  - VLAN's, PVLAN's, switch port security & MAC address filtering, PACL's, VACL's, Dynamic VLAN's, MAC and ARP monitoring, DHCP snooping, DAI, etc
  - ARP spoofing: arpwatch, XArp2, ArpON...
- Free network access vs. 802.1x/EAP (NAC/NAP)
- Disable (if possible) CDP, STP, CDP, PAgP, or VTP, plus non-used ports
- Protection & Detection capabilities

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

47

## VoIP Network Traffic Segregation

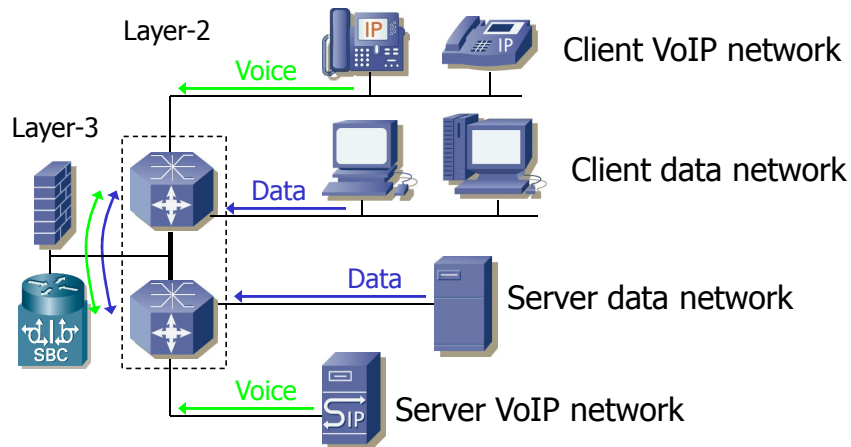
- Logical (or physical) segregation of voice and data traffic
- Relevant security benefits
- Layer-2 segregation (VLAN's) + ...
- Facilitates layer-3 segmentation using ACL's, VoIP-aware firewalls, ALG's or SBC's
- QoS benefits too
- Unified communications paradox?...

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

48



## VoIP Network Traffic Segregation Diagram

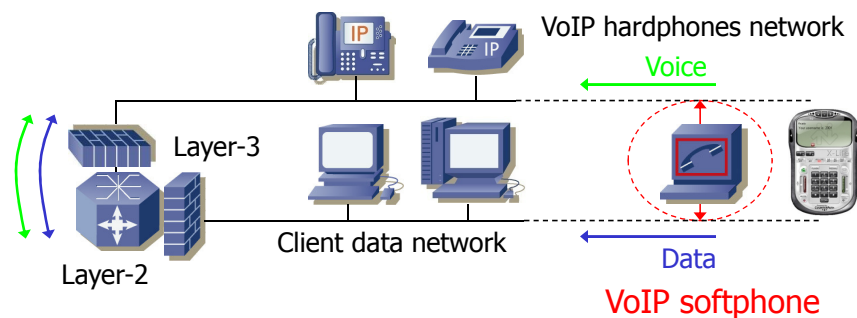


To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

49

## The VoIP Softphone Paradox

- Software-based VoIP phone application
  - Single network; no segregation
- Any other VoIP integrated application



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

50

## Secure VoIP Protocols

- Secure network protocols
  - 802.1x, DNS?, SCP, SNMPv3, HTTPS...
- Signaling authentication and identity
  - Digest (MD5), digital certificates, authenticated identity (RFC 4474)...
- Signaling encryption
  - SIPS (TLS-based SIP) or SIP over DTLS
  - S/MIME
  - VPNs: IPSec or SSL

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

51

## Secure VoIP Protocols (2)

- Media encryption
  - SRTP (Secure RTP) & SRTCP
  - RTP over IPSec
- Key exchange mechanisms
  - SDescriptions
  - MIKEY
  - ZRTP
  - DTLS-SRTP

Other proprietary solutions & Lawful Interception (LI)

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

52

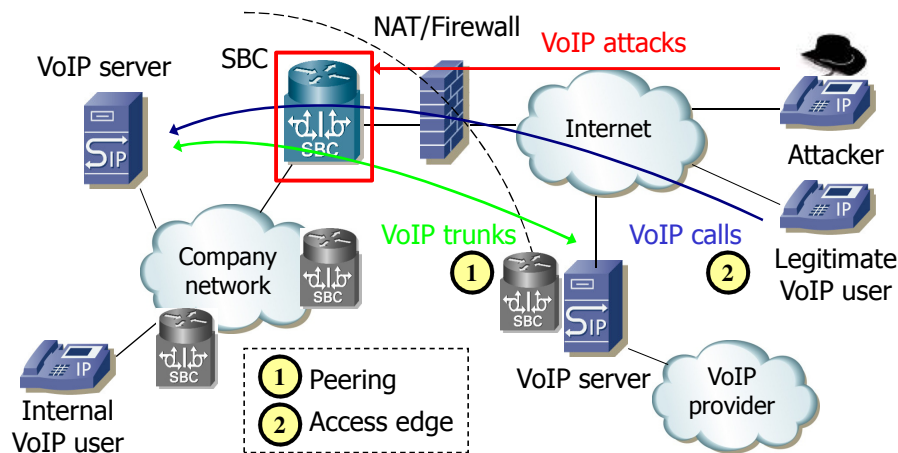
## VoIP Security Devices

- Standard NAT/Firewall issues
  - STUN, TURN, or ICE
- VoIP-aware firewalls
- Application-layer Gateways (ALG's)
- VoIP IDS/IPS
- Session Border Controllers (SBC's)
  - Peering edge and Access edge

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

53

## SBC's



To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

54

## Integrating VoIP into your Security Regime

- Key technology (more than data)
  - Expected availability: 99.999%
- Include it within all security tasks:
  - Incident handling
  - Auditing
  - Penetration testing
    - VoIP & Wardialing

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

55

## Summary

- Data & Voice communications
- Lots of VoIP Attacks...
- VoIP Defenses
  - Secure architecture (defense in-depth and multiple layers), network segregation, secure layer-2 setup & protocols, secure VoIP protocols, VoIP security devices (SBC's)

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

56

## References

- “Practical VoIP Security”. Thomas Porter.
- “Hacking Exposed VoIP”. D. Endler, M. Collier.  
- <http://www.hackingvoip.com>
- “Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures”. Peter Thermos, A. Takanen.
- “LAN Switch Security: What Hackers Know About Your Switches”. Eric Vyncke.
- Blue Box Podcast ([www.blueboxpodcast.com](http://www.blueboxpodcast.com))
- VoIPSA ([www.voipsa.org](http://www.voipsa.org))
- SANS “VoIP Security” course (SEC540)

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

57

## Thanks!!



“To V☺IP or not to V☹IP...  
...esa es la cuestión”



Raúl Siles

- [raul@raulsiles.com](mailto:raul@raulsiles.com)
- [www.raulsiles.com](http://www.raulsiles.com)

To VoIP or not to VoIP, esa es la cuestión © 2009 Raúl Siles

58