

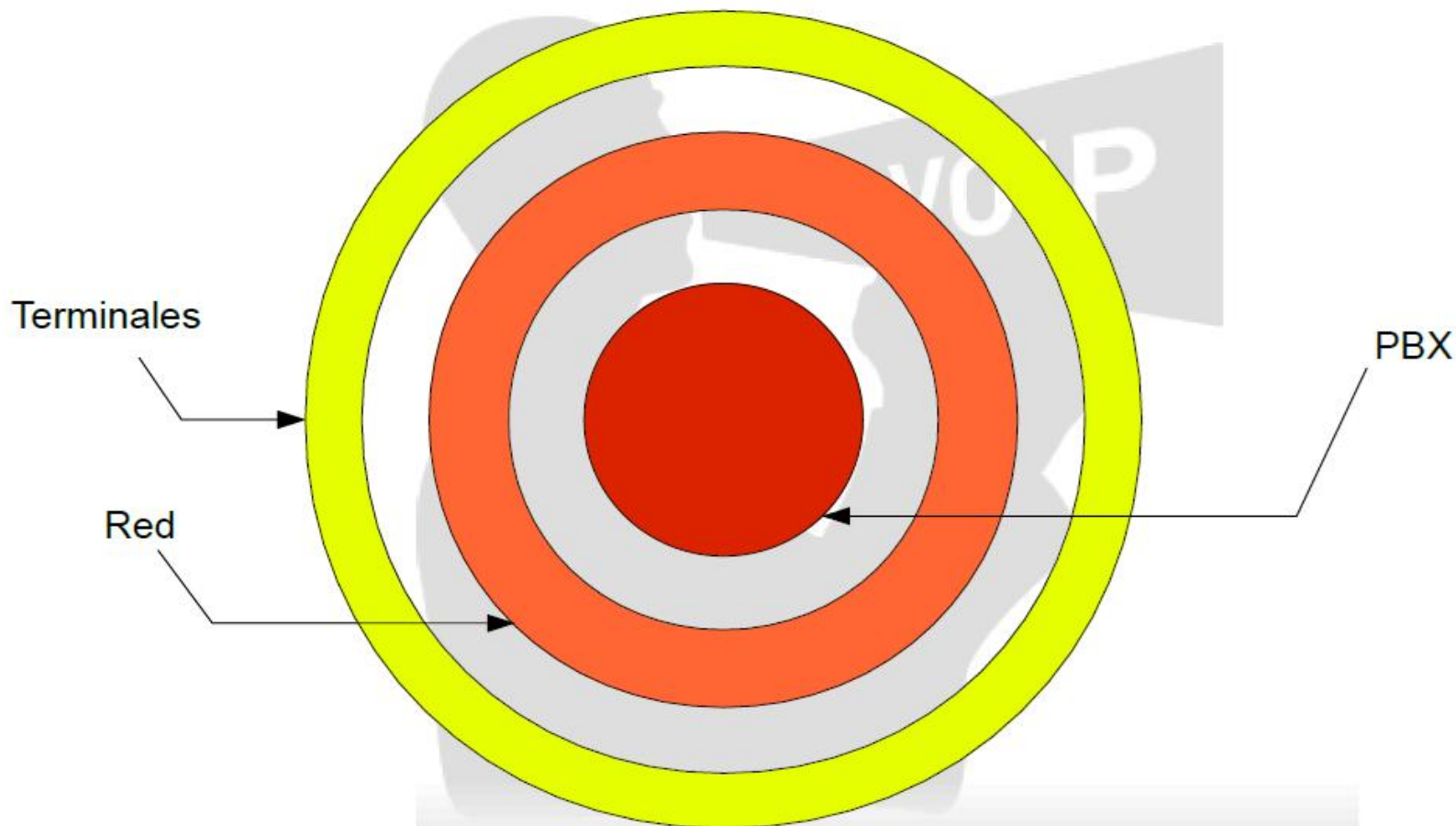


Disertante: Ing. Fernando M. Villares
Rosario – IT FLOSS 2017

El puntapié inicial hacia una noción de seguridad.

- ▶ ¿Han sufrido o conocen sobre algún tipo de ataque a sistemas de comunicaciones?
- ▶ ¿Desde donde espero recibir un ataque?
- ▶ ¿Las comunicaciones son SEGURAS?
 - ¿Es segura la telefonía tradicional?
 - ¿Es seguro el universo de Internet?
- ▶ Análisis Inicial:
 - ¿Sabemos algo?
 - ¿Podemos hacer algo al respecto?

¿Por donde es posible atacar un sistema de VoIP?



Importante: No olvidar el poder de la ingeniería Social sobre la CAPA 8 del modelo OSI (la BIOS).



Ataques:

- Fuzzing
- Flood UDP y RTP
- Fallas de Firmwares y Bugs
- INVITE flood
- Fallos de configuración
- Servicios no desactivados
- Bluetooth / Servicios extras

Fuzzing

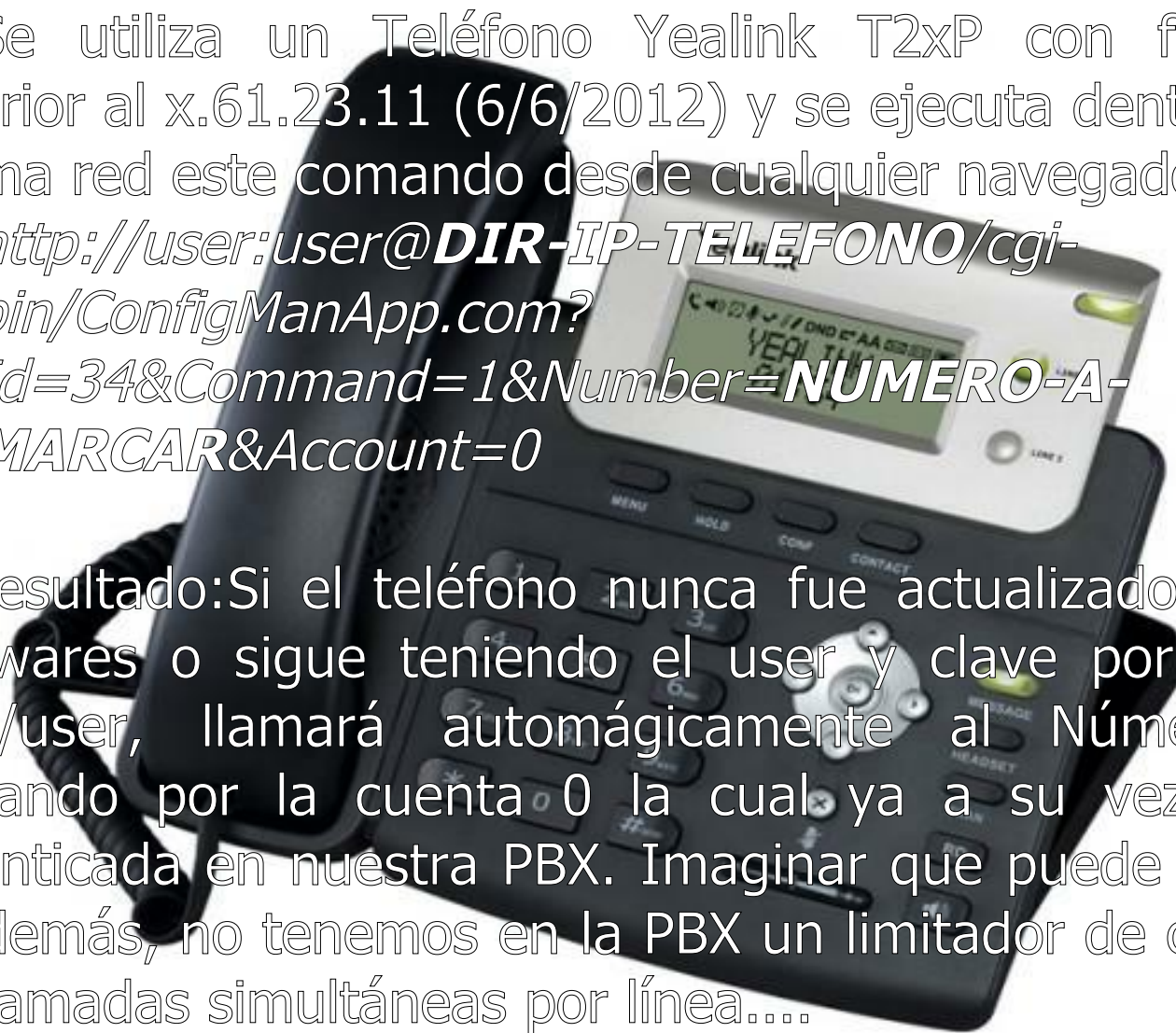
- ▶ Envío de paquetes malformados en busca de errores de programación o bugs.
- ▶ Desbordamientos de buffer, tamaño de variables, fallos de segmentación...
- ▶ Herramientas
 - ▶ PROTON SIP Fuzzer
 - ▶ VoIPER
 - ▶ SiVuS
 - ▶ VOIPPACK (desaparecido)
 - ▶ SIPVICIOUS

Flooding

- ▶ Técnica de Denegación de Servicio (DoS) por inundación.
- ▶ Si se envían miles de paquetes basura no podremos procesar los buenos.
- ▶ Recordemos: packet loss, latencia, jitter...
- ▶ Herramientas:
 - ▶ Inviteflood
 - ▶ Udpflood
 - ▶ Rtpflood
 - ▶ Sipsak
 - ▶ Sipp

Error de capa 8, Bestia ignorante operando Sistema

- ▶ Se utiliza un Teléfono Yealink T2xP con firmware anterior al x.61.23.11 (6/6/2012) y se ejecuta dentro de la misma red este comando desde cualquier navegador web:
 - ▶ *<http://user:user@DIR-IP-TELEFONO/cgi-bin/ConfigManApp.com?Id=34&Command=1&Number=NUMERO-A-MARCAR&Account=0>*
- ▶ Resultado: Si el teléfono nunca fue actualizado en sus firmwares o sigue teniendo el user y clave por default user/user, llamará automáticamente al Número del comando por la cuenta 0 la cual ya a su vez estará autenticada en nuestra PBX. Imaginar que puede suceder si además, no tenemos en la PBX un limitador de cantidad de llamadas simultáneas por línea....



In-Seguridad en terminales

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

► Ataques:

- Flooding / Fuzzing
- Man-In-The-Middle
- Eavesdropping
- Ataques a servicios:

- TFTP / FTP
- DHCP
- SSH
- Apache / PHP / Tomcat
- MariaDB / PostGRE



Seguridad en la red – Routers / Firewalls

- ▶ Muchos routers poseen el protocolo uPnP, que abre puertos automáticamente.
- ▶ Los routers pueden tener vulnerabilidades o ser susceptibles de instalarles RootKits.
- ▶ Muchos proveedores de datos proveen sus propios routers/firewalls con SIP ALG el cual no puede ser desactivado o sin admin permitida
- ▶ Una config correcta es lo más importante!

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 /  
10.10.5.20/ /10.10.5.21//
```

Eavesdropping (I)

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

“Logramos entrar al server, con ese MITM luego usamos Wireshark para capturar y analizar el tráfico.”

Eavesdropping (II)

rtel

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
1161	12.770066232	10.10.7.8	10.10.7.14	UDP	224	15760 → 10003 Len=182

Wireshark · RTP Stream Analysis · wireshark

pcapng_wlp1s0_20160912100115_T0d2YB

10.10.7.10:10054 ↔ 10.10.7.14:10005

Forward

Reverse

Gr

Packet	Sequence	D
1591	23678	
1595	23679	
1598	23680	
1599	23681	
1601	23682	
1603	23683	
1606	23684	
1607	23685	
1609	23686	
1611	23687	
1615	23688	
1617	23689	
1618	23690	
1620	23691	
1623	23692	
1624	23693	
1626	23694	
1629	23695	
1631	23696	
1633	23697	
1634	23698	
1636	23699	
1638	23700	
1641	23701	
1643	23702	
1645	23703	
1646	23704	
1648	23705	
1651	23706	
1653	23707	
1655	23708	

Forward

Reverse

SSRC

Max Delta

Max Jitter

Mean Jitter

Max Skew

RTP Packets

Expected

Lost

Seq Errs

Duration

Clock Drift

Freq Drift

0x0199319c

90.52 ms @ 2705

7.74 ms

0.92 ms

-67.22 ms

716

716

0 (0.00 %)

0

14.30 s

-806 ms

7549 Hz (-5.64 %)

Reverse

SSRC

Max Delta

Max Jitter

Mean Jitter

Max Skew

RTP Packets

Expected

Lost

Seq Errs

Duration

Clock Drift

Freq Drift

0x0199319c

0.00 ms @ 0

0.00 ms

0.00 ms

0.00 ms

0

1

1 (100.00 %)

0

0.00 s

0 ms

1 Hz (0.00 %)

1 streams found.

Wireshark · RTP Player

○ Jitter Drops

◇ Wrong Timestamps

▲ Inserted Silence

Source Address	Source Port	Destination Address	Destination Port	SSRC	Setup Frame	Packets	Time Span (s)	Sample Rate
10.10.7.10	10054	10.10.7.14	10005	0x0199319c	1575	716	23.9 - 38.2 (14.3)	8000

▶

■

Jitter Buffer: 50

Playback Timing: jitter Buffer

☐ Time of Day

Close

Help

wireshark_pcapng_wlp1s0_20160912100115_T0d2YB

Packets: 3093 · Displayed: 3093 (100.0%)

Profile: Default

Ataques a servicios

- ▶ Normalmente en una PBX Asterisk se utiliza:
 - TFTP o FTP para aprovisionamiento de fonos.
 - DHCP para obtener una IP.
 - Email para el servicio de fax y Voicemail
- ▶ Si desenchufamos un teléfono y esnifeamos la red, podemos saber que archivo pide. ¡Y pedirlo nosotros, usando la herramienta TFTPTheft!
- ▶ Podemos agotar las direcciones DHCP, para que los fonos no tengan IP, no pudiendo funcionar.
- ▶ Puedo atacar el server de email via un exploit y lograr control del sistema o saturar sus recursos.
- ▶ Ejemplo de agotamiento de direcciones IP:
`# dhcpx -i eth0 -vv -D 10.10.5.254`

- ▶ Consecuencias:
 - Privacidad al descubierto.
 - Interrupción del servicio.
 - Configuraciones, contraseñas...
ial descubierto!
- ▶ ¿Cómo nos defendemos?
 - Separar la red en distintas VLAN (voz y datos desde los switches o routers)
 - Audio y signalling cifrado: SRTP, TLS
 - Sistemas de mitigación de DoS.

► Ataques:

- Flooding.
- Ataques de peticiones remotas.
- Cracking de passwords.
- REGISTER hijacking.
- Exploits.
- Errores de configuración.
- Implementadores de “garage”.
- Ing. Social en Sistemas OOTB.

Ataques de peticiones remotas de llamadas.

- ▶ Ataques de gran volumen realizados por bots o maquinas zombies, no se centran en realizar llamadas “per se” sino en establecer cargos de interconexión ya que los proveedores de telecomunicaciones entre ellos se cobran mínimos cargos de interconexión.
- ▶ Banear rangos de IP no suele funcionar porque provienen de miles de IP diferentes y en zonas diferentes.
- ▶ Motivación: ganar dinero por cargos de conexión, si se establece la llamada o es a un número premium mucho mejor!!!

Ataques de peticiones remotas de llamadas: PASOS

- (1) Escaneo de IP y ports.
- (2) Probar a enviar una petición de llamada anónima a un número de teléfono de la red beneficiaria.
- (3) Búsqueda de una cuenta SIP vulnerable con la que registrarse.
- (4) Registro como softphone, llamadas a números donde se encuentra la red beneficiada, si el número no descuelga, algún intermedio descolgará y cobrará llamada internacional, esto no es legal, pero es tremendamente difícil de detectar y denunciar.
- (5) Se detecta número de canales salientes disponibles, para maximizar el número de llamadas por tiempo y minimizar el número de peticiones a realizar para evitar ser detectado.

Crackeando los passwords en el protocolo SIP

- ▶ Sistema de autenticación mediante HTTP-Digest (RFC2617):
 - 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.
- ▶ iiEste proceso se hace 'casi' con cada mensaje!!
- ▶ El algoritmo usado es md5, se puede romper.
- ▶ Se suelen usar contraseñas muy simples...

Crackeando los passwords en el protocolo SIP (II)

- ▶ Para romper el cifrado necesitamos capturar los paquetes que viajan en ambos sentidos en el momento de la autenticación mediante HTTP-Digest.
- ▶ Man In The Middle (M.I.T.M.)
- ▶ Herramientas: SIPcrack, SIPdump, John The Ripper (pago), Cain & Abel
- ▶ Ejemplo (usando sipdump y sipcrack):

```
#sipdump -i eth0 captura.dump |  
./sipcrack -w DICC.TXT captura.dump
```

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 10.10.5.250 10.10.5.250  
secuestrador@10.10.7.30 -u 200 -p mipass
```

Exploits

- ▶ Errores en la programación que pueden llevar a desbordamientos de buffer, escritura en memoria inválida, fallos de segmentación...
- ▶ Ciertos invites malformados en asterisk 1.8 causaban deadlocks, 1.4.0 daba un core dump con content-length<0.
- ▶ El Xlite 1103 al enviarle un INVITE con el 'Content-Length' ≥ 1073741823 se pone a consumir RAM y decae el rendimiento del sistema.
- ▶ Asterisk es Software Libre, mucha gente lo estudia y por tanto sus fallos se corrigen muy pronto.
- ▶ Pero, ¿Qué pasa con las BlackBox privativas? Eolos, Cisco, Avaya, 3Cx, Denwa, M\$ Lync (LoL) etc.

Errores en las configuraciones (siempre Capa 8)

- ▶ `allowguest=no` ; permite o rechaza las comunicaciones de invitados (por defecto es yes)
- ▶ Contextos y permisos adecuados al nivel de privilegios del usuario.
- ▶ T: Permite que el usuario llamado transfiera una llamada marcando las teclas de transferencia ciega de `features.conf`.
- ▶ No limitar o controlar el número máximo de llamadas por usuario o troncal de la PBX.
- ▶ IN-seguridad en los canales de conferencias remotos y DISA (vieron MR ROBOT, temporada 2?)

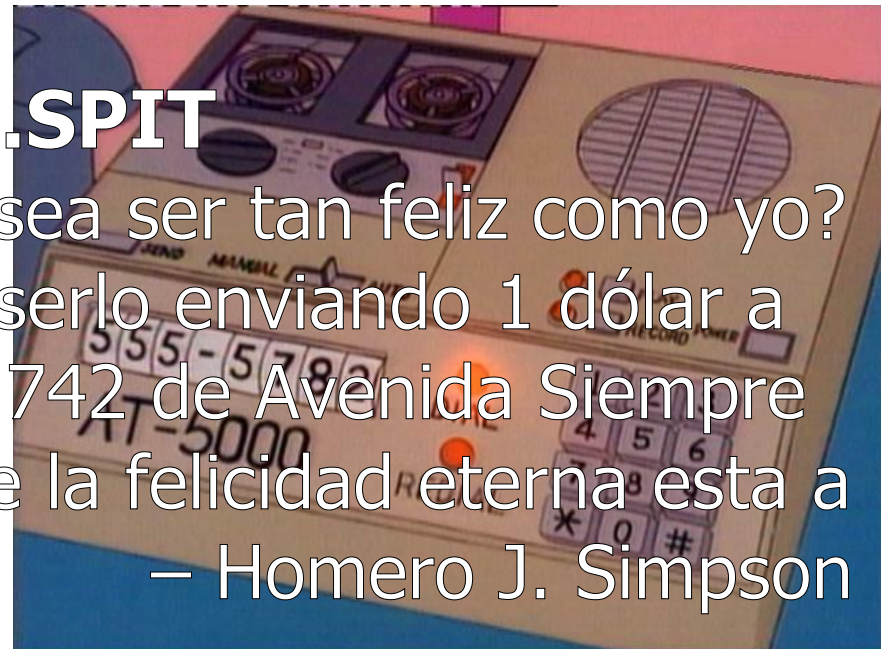
- ▶ Consecuencias:
 - Interrupción TOTAL o parcial del servicio.
 - Toll fraud / Fraude de llamadas.
 - 'Robo' de llamadas.
 - Escuchas INDEBIDAS.
- ▶ ¿Cómo nos defendemos?
 - Señalización cifrada.
 - SIP sobre TCP/TLS.
 - Activar solo los servicios necesarios.
 - Firewalls/sistemas de mitigación de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

► Si hemos conseguido la clave del usuario podemos hacer de todo:

- Transferirle llamadas
- Colgarle llamadas
- Otras posibles molestias...xD...

► SPAM en VoIP...SPIT

- Hola amigo! Desea ser tan feliz como yo? Pues ya puede serlo enviando 1 dólar a Hombre feliz al 742 de Avenida Siempre Viva, no lo dude la felicidad eterna esta a solo un dólar!
- Homero J. Simpson



Algunas Herramientas...

- ▶ Sipsak y SIPP son Herramientas estándar para benchmarking y testing de SIP, también las podemos usar para hacer flooding :-)
- ▶ Uso: #sipsak -F -s sip:intelix@172.16.20.100
#sipp 172.16.20.100 (pulsar +++)
- ▶ Flooding (enviamos 1.000.000 de paquetes):
#udpflood 192.168.1.3 192.168.1.251 9 5060 1000000
#inviteflood eth0 200 ippbx.local 192.168.1.21 1000000
#rtpflood 192.168.1.3 192.168.1.251 9 16384 1000000
15000 2000 1886986910
- ▶ Cain & Abel: Herramienta completa de cracking con funcionalidades de VoIP.
 - ▶ ARP Poisoning con 1 click
 - ▶ iEavesdropping con cualquier codec!

Algunas Herramientas (II)...

- ▶ SiVuS: Herramienta de auditoría, seguridad y generación de tráfico SIP, permite testear dispositivos SIP en busca de vulnerabilidades.
- ▶ SipVicious, Conjunto de herramientas de seguridad en VoIP:
 - ▶ Svmmap (escaneador SIP)
 - ▶ Svcrack (crackeador de contraseñas)
 - ▶ Svwat (enumerador de extensiones)
- ▶ Uso:
 - ▶ `svmmap.py 192.168.1.1-254`
 - ▶ `svwat.py -e200-299 192.168.1.111`
 - ▶ `svcrack.py -u200 dict.dat 192.168.1.111`

Algunas Herramientas (III)...

- ▶ Voiper: Potente fuzzer con muchos casos de prueba
- ▶ Se usa en como herramienta de testing para detectar fallos en software y hardware.
- ▶ Uso:
 - ▶ `#python fuzzer.py -f SIPInviteCommonFuzzer -i 192.168.3.101 -p 5060 -a sessions/scen1 -c 0`
 - ▶ `#python fuzzer.py -f SIPInviteCommonFuzzer -c 2 -i 192.168.3.101 -p 5060 -a sessions/scen2 -m 1024`
 - ▶ `#python torturer.py -i 192.168.1.2 -p 5060 -c 0 -t invalid`

Análisis final de Seguridad en Comunicaciones IP...

- ▶ En el mundo del SIP sobre UDP y el RTP la VoIP es INSEGURA y punto.
- ▶ Pero, es necesario cierto acceso a la red para poder comprometer la seguridad.
- ▶ Entonces securizar hoy es no lamentar mañana, por ejemplo por medio de:
 - **Túneles VPN para enlaces a través de Internet.**
 - **Distintas VLAN para voz y datos.**
 - **Contraseñas robustas, SIP TLS, SRTP.**
 - **Servicios más seguros, DHCP por MAC, 802.1x, Switches Layer 2/3.**
 - **Firewalls y Sistemas de IDS/IPS.**

Seguridad en comunicaciones VoIP con Asterisk

- ▶ Asterisk en sus ramas desde la 1.8, hasta la actual 14, soporta cifrado de medios y seguridad en canales SIP a través del protocolo SRTP para el sonido y de SIP sobre TLS para la señalización.
- ▶ Asterisk soporta certificados de firma digital, y cifrado AES-128 en su protocolo nativo **IAX2** lo cual lo convierte en una opción muy atractiva para mantener la privacidad de la información que circula desde y hacia el servidor.
- ▶ Se debe tener muchísimo cuidado al securizar los servidores a usar, ya sea por medio de firewalls de filtrado de paquetes, medios seguros de control de acceso y sistemas de auditoría. Por ejemplo: **Fail2Ban**

TLS y SRTP en Asterisk

Generación de certificados para uso en TLS con asterisk:

Asterisk posee su propio script para generar certificados digitales...

Generación de CA y certificado de servidor:

```
#./ast_tls_cert -C 192.168.2.100 -O "INTELIX" -d /etc/asterisk/keys
```

Generación de certificados de clientes:

```
#./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k  
/etc/asterisk/keys/ca.key -C 192.168.2.1 -O "INTELIX" -d  
/etc/asterisk/keys -o yealink1
```

Cada certificado tiene validez de 1 año y llaves de 4096 bits.

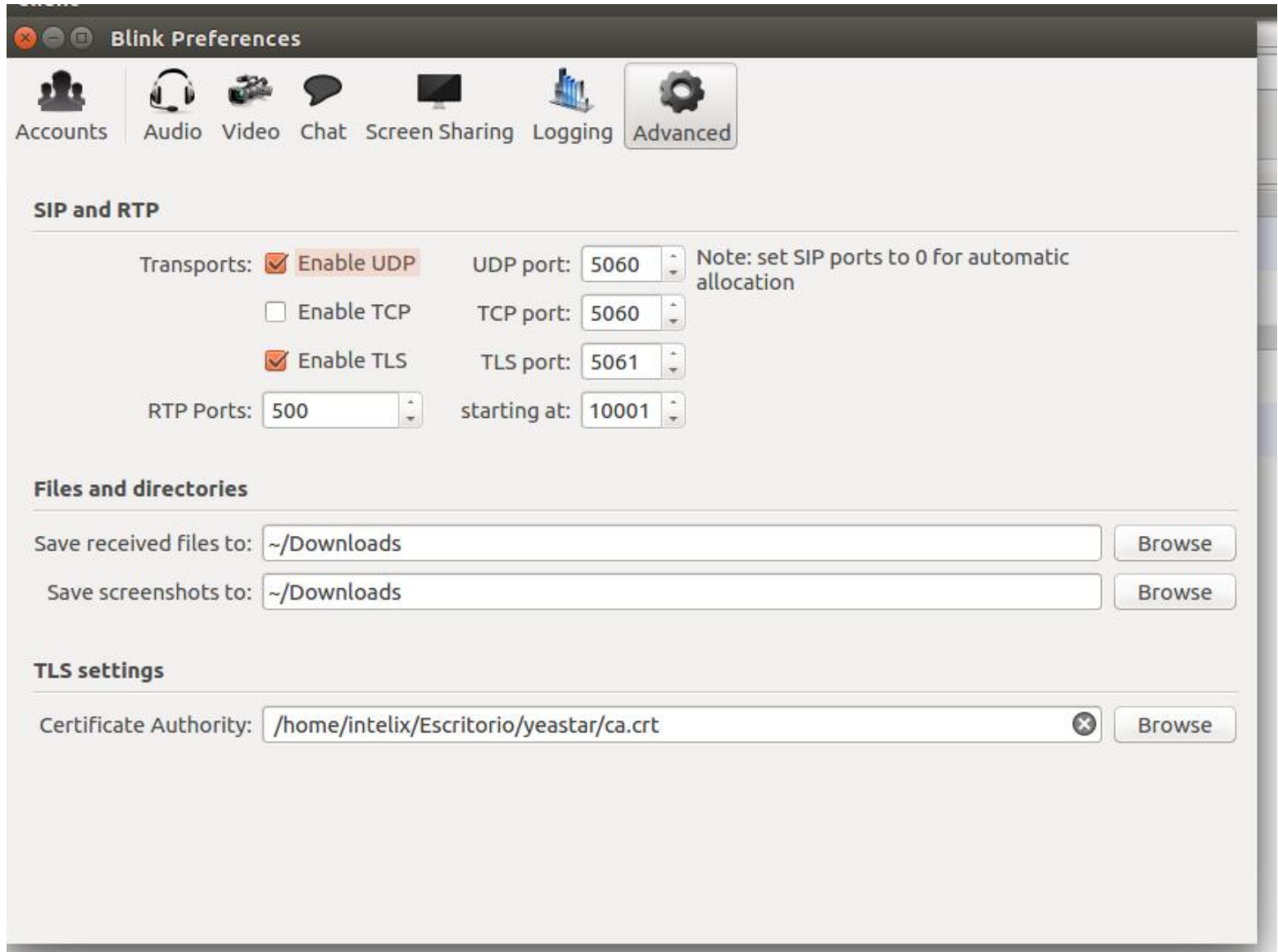
TLS y SRTP en Asterisk

Configuración de TLS en Asterisk 11 y + (sip.conf):

```
tlsenable=yes  
tlsbindaddr=0.0.0.0:5061  
tlscertfile=/etc/asterisk/keys/asterisk.pem  
tlscapath=/etc/asterisk/keys/ca.crt  
tlscapath=/etc/asterisk/keys  
tlsdontverifyserver=no  
tlsverifyclient=yes  
tlsignorecommonname=no  
tlscipher=ALL  
tlsclientmethod=tlsv1
```

Configuración (sip.conf) en cada usuario:

```
encryption=yes  
transport=tls
```



Blink Preferences

Accounts Audio Video Chat Screen Sharing Logging **Advanced**

SIP and RTP

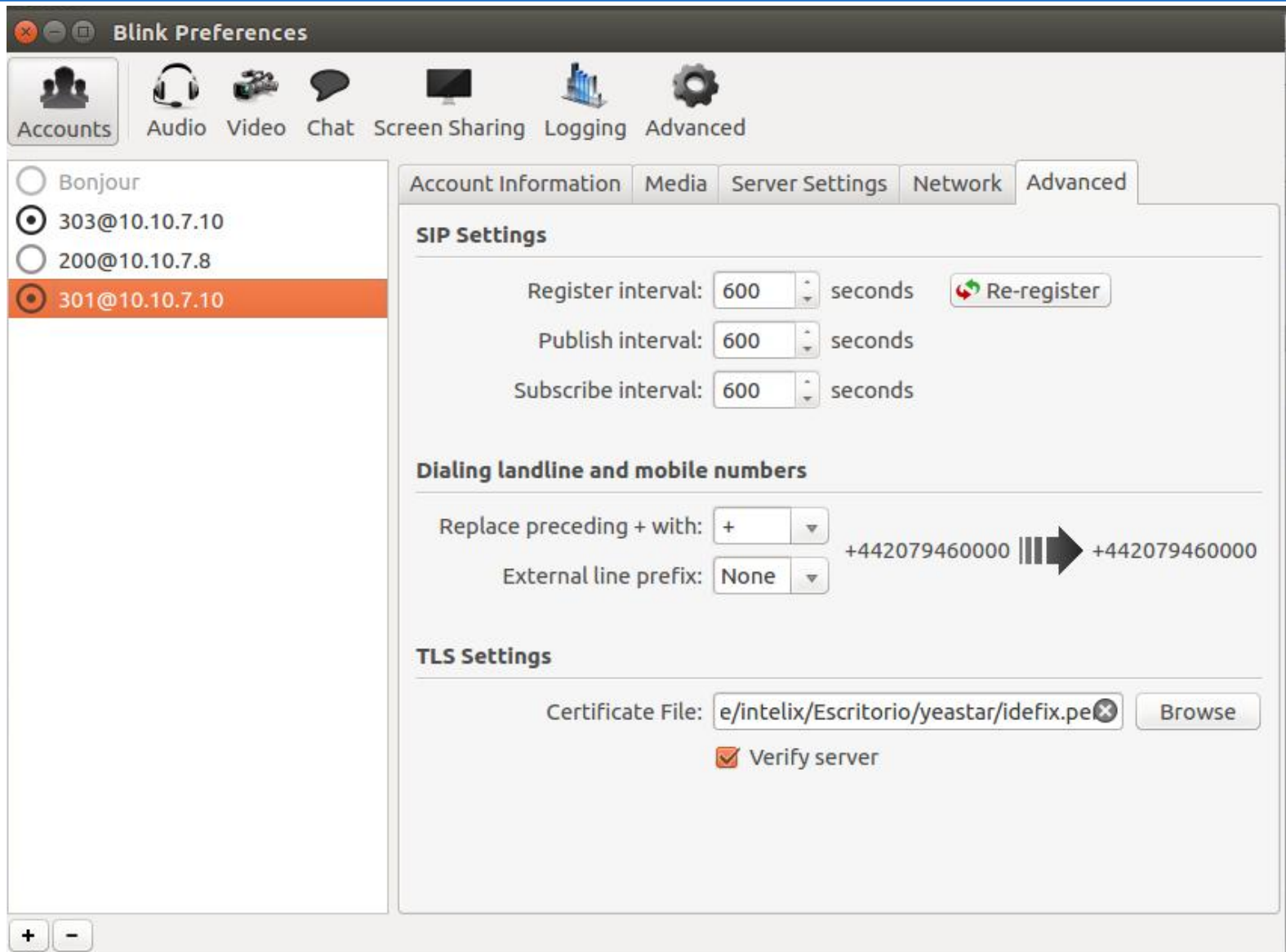
Transports: ☒ **Enable UDP** UDP port: 5060 Note: set SIP ports to 0 for automatic allocation
☐ Enable TCP TCP port: 5060
☒ **Enable TLS** TLS port: 5061
 RTP Ports: 500 starting at: 10001

Files and directories

Save received files to: ~/Downloads **Browse**
 Save screenshots to: ~/Downloads **Browse**

TLS settings

Certificate Authority: /home/intelix/Escritorio/yeastar/ca.crt **Browse**



Blink Preferences

Accounts Audio Video Chat Screen Sharing Logging Advanced

Accounts

- ☐ Bonjour
- ☒ 303@10.10.7.10
- ☐ 200@10.10.7.8
- ☒ 301@10.10.7.10

Account Information Media Server Settings Network **Advanced**

SIP Settings

Register interval: 600 seconds [Re-register](#)

Publish interval: 600 seconds

Subscribe interval: 600 seconds

Dialing landline and mobile numbers

Replace preceding + with: +

External line prefix: None

+442079460000 ||| ➡ +442079460000

TLS Settings

Certificate File: e/intelix/Escritorio/yeastar/idefix.pem [Browse](#)

☒ Verify server

Salir
Yealink T46G

Estado |
 Cuenta |
 Red |
 Tecla DSS |
 Funciones |
 Configuración |
 Directorio |
 Seguridad

Contraseña

Certificados de confianza

Certificados servidor

Índice	Emitido a	Emitido por	Expiración	del
1	Asterisk Private CA	INTELIX	Sep 11 18:45:06 2017 GMT	<input type="checkbox"/>
2				<input type="checkbox"/>
3				<input type="checkbox"/>
4				<input type="checkbox"/>
5				<input type="checkbox"/>
6				<input type="checkbox"/>
7				<input type="checkbox"/>
8				<input type="checkbox"/>
9				<input type="checkbox"/>
10				<input type="checkbox"/>

del

Solo acepta certificados de confianza

?

Validación de nombre común

?

Certificados CA

?

Nota

Trusted Certificates
La lista de certificados confiables.

You can click here to get more guides.

Importar certificado de confianza (.cer) ?

Cargar archivos de certificados confiables

No se seleccionó un archivo

Yealink

T46G

Estado

Cuenta

Red

Tecla DSS

Funciones

Configuración

Directorio

Seguridad

Contraseña

Certificados de confianza

Certificados servidor

Emitido a	Emitido por	Expiración	del
10.10.7.4	INTELIX	Sep 12 13:07:35 2017 GMT	<input type="checkbox"/>

Certificados de dispositivo

Certificados personalizar ?

Importar certificado de servidor ?

Cargar archivo de certificado de servidor

Examinar...

No se seleccionó un archivo

Cargar

Confirmar

Cancelar

Nota

Server Certificates

Lista de certificados del servidor

You can click here to get more guides.

TLS y SRTP YEALINK T46G

Salir
Yealink | T46G

Estado **Cuenta** Red Tecla DSS Funciones Configurac Directorio Seguridad

Registrar

Básico

Códec

Avanzado

Cuenta Cuenta 5 ?

Estado del registro	Registrado	
Línea activa	Activado	?
Etiqueta	<input type="text" value="300"/>	?
Nombre para mostrar	<input type="text" value="300"/>	?
Nombre de registro	<input type="text" value="300"/>	?
Nombre de usuario	<input type="text" value="300"/>	?
Contraseña	<input type="password" value="....."/>	?
Servidor SIP 1 ?		
Host servidor	<input type="text" value="10.10.7.10"/> ?	Puerto <input type="text" value="5061"/>
Transporte	TLS	?
Expiración de servidor	<input type="text" value="3600"/>	?
Reintentos de servidor	<input type="text" value="3"/>	?
Servidor SIP2 ?		
Host servidor	<input type="text" value=""/> ?	Puerto <input type="text" value="5060"/>
Transporte	TCP	?
Expiración de servidor	<input type="text" value="3600"/>	?
Reintentos de servidor	<input type="text" value="3"/>	?

Nota

Display Name
El nombre de para mostrar.

Nombre de registro
El ID de suscripción de servicio SIP será usado para autenticación.

User Name
Cuenta de Usuario, proporcionada por el proveedor de servicio VoIP

NAT Traversal
Define si el servidor STUN estará activo o no.

You can click here to get more guides.

BIBLIOGRAFÍA CONSULTADA

- ▶ *Internet Engineering Task Force (www.ietf.org) RFC 2401-2764-2709-2411-2521-2685-2833*
- ▶ *Recursos VoIP – Web Page – (www.recursosvoip.com)*
- ▶ *Cisco VoIP White Papers - www.cisco.com*
- ▶ *Voip-Info Web Page – www.voip-info.org*
- ▶ *Digium Home Pages – www.asterisk.org / www.digium.com*
- ▶ *International Telecommunication Union WebPage - www.itu.int*
- ▶ *Voip Novatos - www.voipnovatos.es*
- ▶ *FreePBX & TrixBos forums - www.trixbox.org / www.freepbx.org*
- ▶ *Irontec Soluciones Linux para empresas - www.irontec.com*
- ▶ *Asterisk The definitive guide 3da. Edición. - McGraw Hill 2011*
- ▶ *Nerd Vittles Home Page - www.nerdvittles.com*
- ▶ *Sinologic.net/Avanzada 7 – Elio Rojano - www.sinologic.net*
- ▶ *Commlogik Corporation - www.commlogik.com*
- ▶ *Elastix PBX Forums - www.elastix.org*
- ▶ *Polycom Reference Guides and manuals - www.polycom.com*
- ▶ *Asterisk Guru Home Page - www.asteriskguru.com*
- ▶ *Asterisk Docs - www.asteriskdocs.com*
- ▶ *Seguridad en Voip - Saúl Ibarra Corretgé - www.saghul.net*
- ▶ *Asterisk MX Blog – Christian Cabrera – www.asteriskmx.com*

LICENCIA DE ESTA PRESENTACIÓN



Ingeniería & Telecomunicaciones

Autor: Ing. Fernando M. Villares Terán 03/2017

**Bajo licencia Creative Commons <http://creativecommons.org/>
Atribución-CompartirIgual 2.5 Argentina (CC BY-SA 2.5)**

**Consultas: contacto@intelix.com.ar
www.intelix.com.ar**

***TODAS LAS MARCAS REGISTRADAS NOMBRADAS O UTILIZADAS
EN ESTA PRESENTACIÓN SON PROPIEDAD DE SUS RESPECTIVOS
DUEÑOS Y NO DEBEN SER USADAS SIN LA CORRESPONDIENTE
AUTORIZACIÓN DE LOS MISMOS.***