LA SEGURIDAD EN SIP DEBE EMPEZAR A PREOCUPARNOS

06 de Octubre de 2011
Voip2day

Alberto Sagredo Castro
www.voipnovatos.es

¿SIP es inseguro?

Seguridad SIP

- SIP como tal no es inseguro ni inseguro. Tiene ciertas brechas de seguridad como ataques por fuerza bruta y fragilidad por autenticación MD5
- “El sistema seguro es aquel que está aislado de Internet”
- Malas configuraciones realizadas por clientes . Aperturas de puertos sin saber..

Securizar SIP en Asterisk

- Comentado ya en otros sitios e incluso charlas ☺
- ACLs
- Cambiar SIP de puerto
- Dominios SIP
- No permitir INVITES externos

Securizar SIP en Asterisk (II)

- Alwaysauthreject=yes
- No permitir INVITES invitado
- Password fuertes
- NO DMZ
- Fail2ban
- VPN

Securizar SIP en Asterisk (II)

- Recogidos en :
- http://www.voipnovatos.es/item/2009/08/cmo-proteger-tu-asterisk-frente-a-ataques

¿Estamos preocupados por la seguridad en SIP?

- Busquemos en Google
- 34.600.000 resultados @ 03/10/2011 !
- Asterisk tienen 13.600.000 resultados
- Nada que hacer contra David Guetta que tiene 153.000.000
- Pero vemos que algo si que preocupa…

¿Estamos preocupados por la seguridad en SIP? (II)

- Desde 2006 hay posts en foros , listas de correo preocupados por SRTP, SIP sobre TLS, pero en su día eran experimentos. Versiones de asterisk con soporte SRTP que no funcionaban… pero era

¿Estamos preocupados por la seguridad en SIP? (III)

- Tenemos disponible aplicaciones que si funcionen para dotar de más seguridad a nuestros sistemas en SIP..
- Desde hace años Openser/Kamailio
- ¿Es muy complicado?

SIP TLS con Kamailio

```
disable_tls = 0
listen = tls:10.16.10.7:5061
#tls_verify_server = 1
tls_verify_client = 1
tls_require_client_certificate = 0
tls_method = TLSv1
tls_certificate =
"/usr/local/etc/openser/tls/openSer/openSer-
cert.pem"
tls_private_key =
"/usr/local/etc/openser/tls/openSer/openSer-
privkey.pem"
tls_ca_list =
"/usr/local/etc/openser/tls/openSer/openSer-
calist.pem
```

Asterisk en la pre-crisis con TLS

- Se usaba Openser como frontend para SIP TLS ya que el soporte de Asterisk por aquel entonces era malo malísimo.
- Solución que funcionaba, pero que nadie usaba
- ¿Proveedores que oferten SIP con TLS? 1,2,3 responda otra vez….

Webs con HTTPs

- En el origen del Internet… a quien le preocupaba:
- Spoofing
- Man in the middle
- Sniffers
- Puntos de acceso público Wifi
- Redes no controladas

Webs con HTTPs

- Con el tiempo todo esto ha cambiado.
- ¿Quién se atreve a hacer login en una página del banco desde un hotspot sin https?
- Todos sabemos que siempre hay gente..

Chuck Norris lo haría

SSL/TLS

- Pero no todos somos tan “valientes” como Chuck Norris.
- Tenemos que tomar precauciones y una disponible hoy en día es SSL/TLS

¿Qué es TLS?

- **Secure Sockets Layer** (**SSL**; protocolo de capa de conexión segura) y su sucesor **Transport Layer Security** (**TLS**; seguridad de la capa de transporte) son protocolos criptográficosque proporcionan comunicaciones seguras por una red, comúnmente Internet.día es SSL/TLS

¿Qué es TLS?

- SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

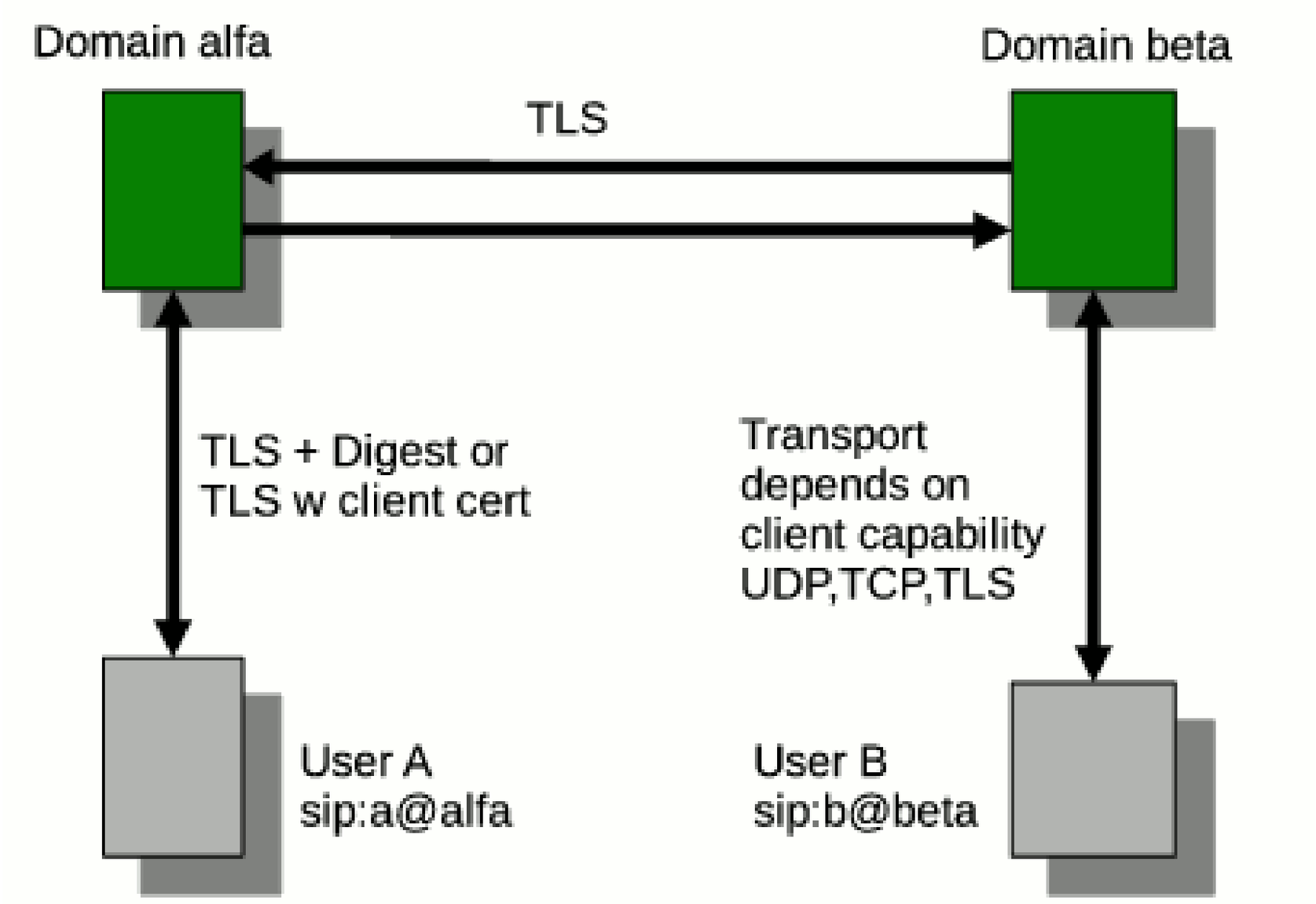
¿Qué es TLS?

- SSL implica una serie de fases básicas:
- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales
- Cifrado del tráfico basado en cifrado simétrico

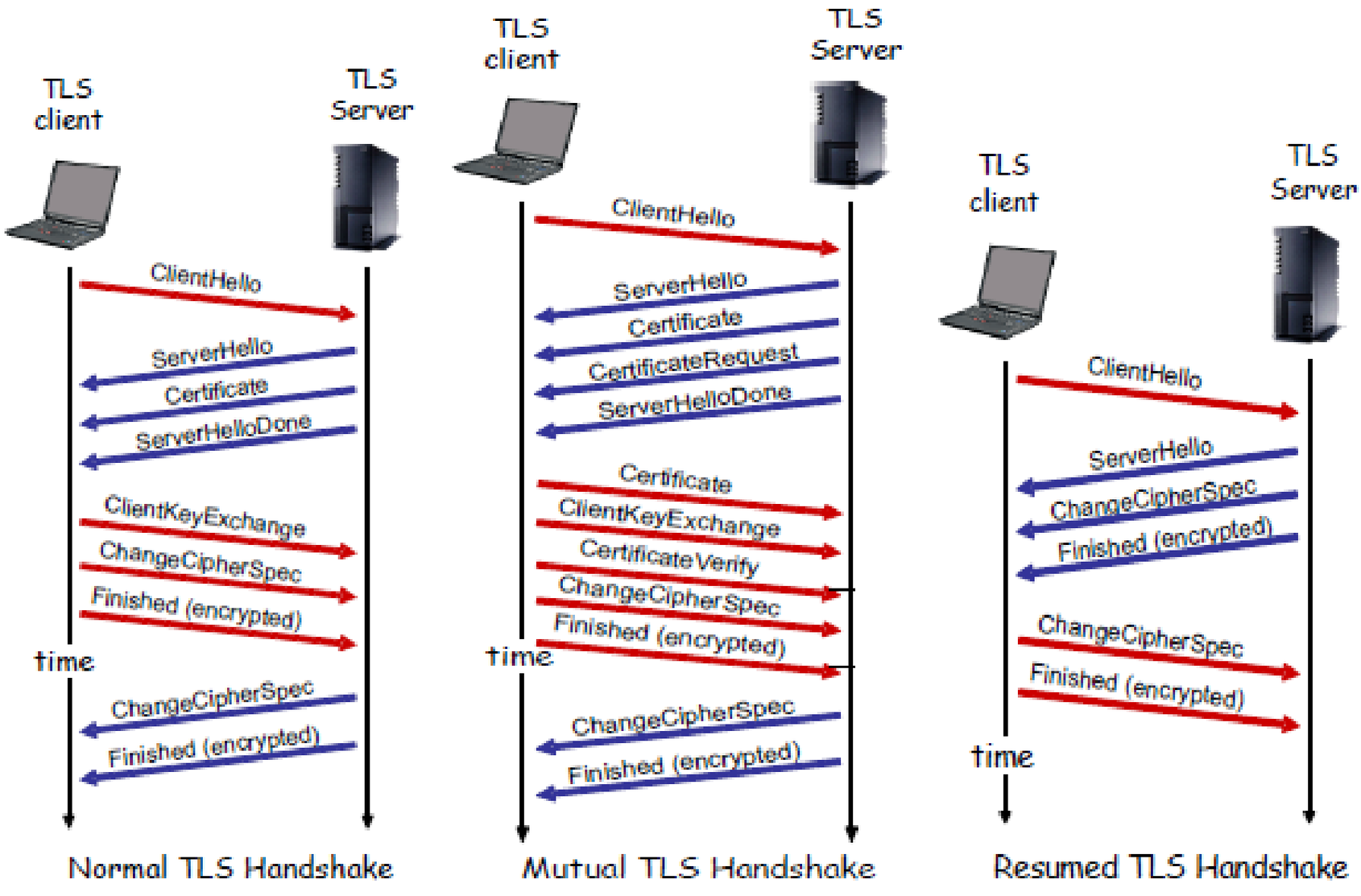
Sesión en SIP TLS

- El cliente SIP se conecta al Proxy
- El cliente SIP pide sesión TLS al proxy
- El proxy le manda su certificado público
- El cliente valida el certificado
- Cliente y proxy intercambian sus claves de sesión
- La sesión es encriptada con esa clave de sesión

Sesión en SIP TLS



Sesión en SIP TLS



Usemos SIP con TLS!

Consideraciones

- TLS necesitará algo más de CPU. ¿Cuánto? ¿Cómo no lo usa nadie en SIP no hay casi estudios todavía ? ☺
- Por lo general si tienes pocas extensiones no necesitarás usar más CPU para este menester.
- Pruebalo! . Es la mejor manera de saber como responde.
- Siempre es buen momento para montar una granja de servidores! ☺

Consideraciones

- Estudio interesante de la Universidad de Columbia
- https://mice.cs.columbia.edu/getTechreport.php?techreportID=602&format=pdf&

Perfomance con SRTP

- Se añaden sobre-cabeceras.

RTP payload length (bytes)		16	32	64	128	256	512	1024	2048
Throughput (megabits/second)	encryption only	183	213	223	238	243	245	248	249
	encryption and authentication	37.6	64.0	88.3	119	142	159	168	173
	authentication only	38.8	88.3	138.4	233	341	436	512	569

Throughput con SIP/TLS

- Se reduce aproximadamente al 50 %. Vs UDP
- Sobrecarga cabeceras hasta un 75 % vs UDP
- Mejora usar conexiones persistentes TLS (Aastra lo soporta)
- Coste de CPU de un 13 a un 58 % más.

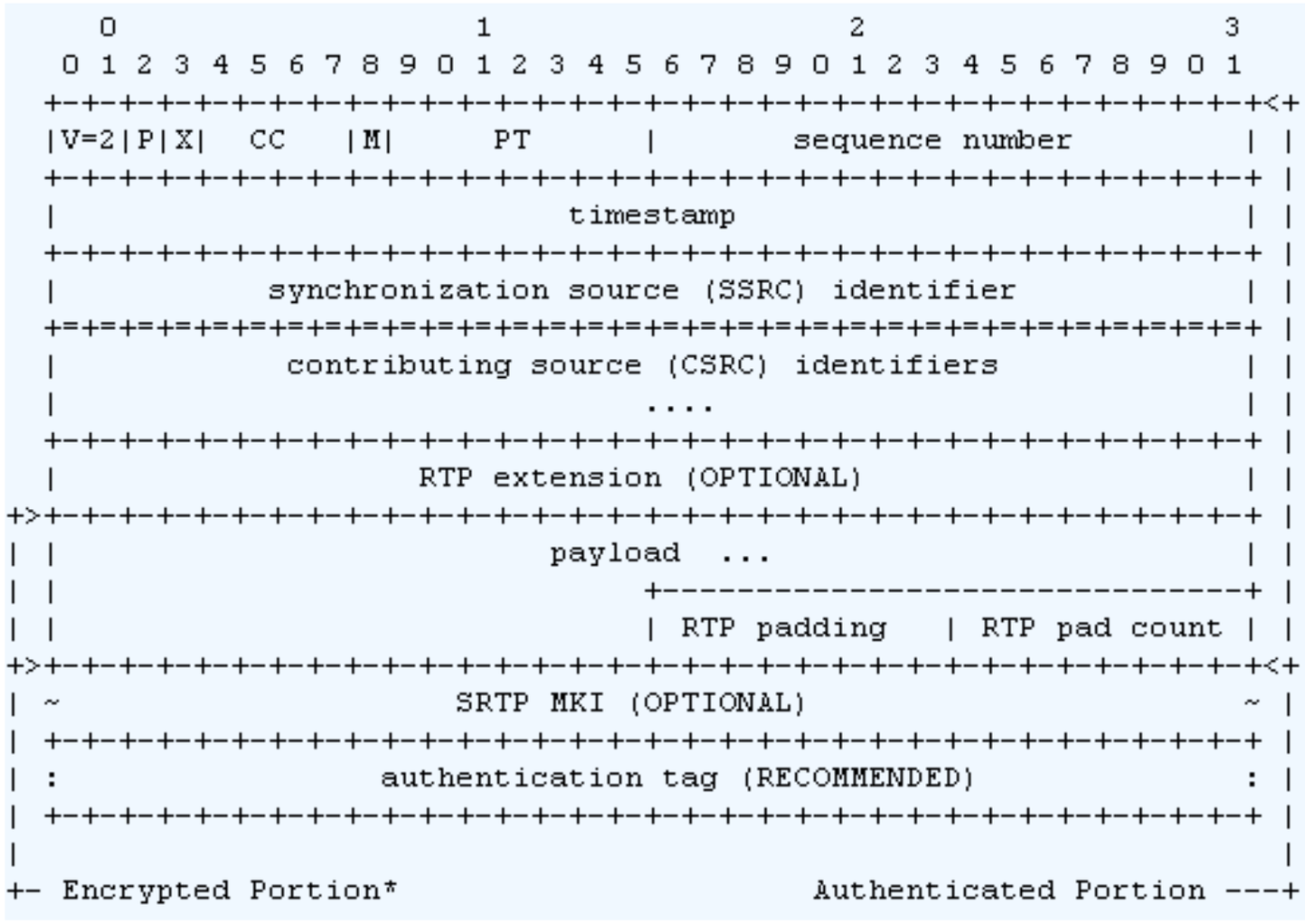
¿Y la voz?

- SRTP es nuestro amigo. Añade cabeceras al SDP con la clave simétrica a encriptar. Interesante que esto vaya sobre TLS para que tampoco se vea la clave intercambiada.

- Otras alternativas ZRTP
- http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5318963

Perfomance con SRTP

- Se añaden sobre-cabeceras.

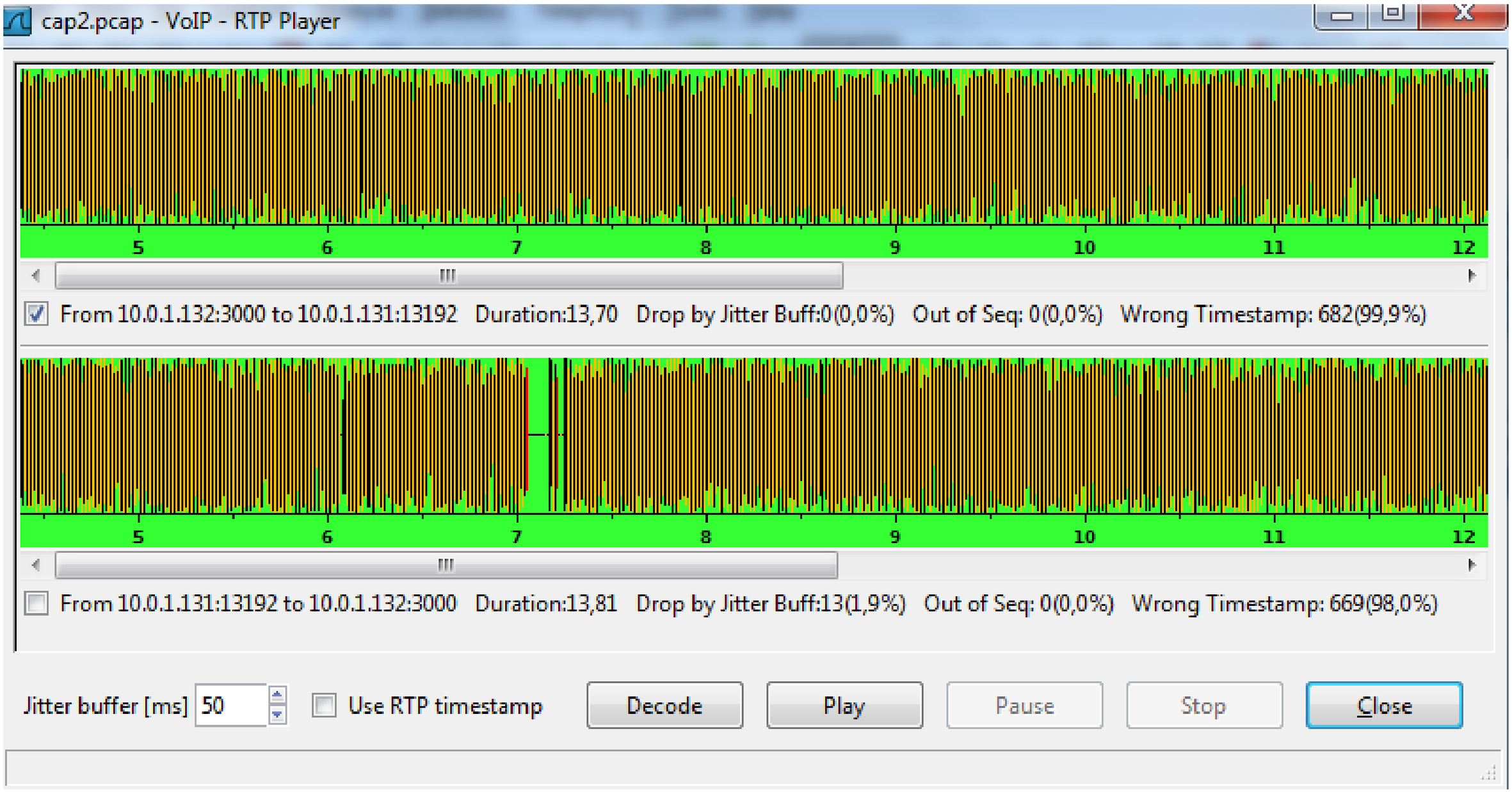


¿Qué cambia?

```
c=IN IP4 10.0.1.132

t=0 0

m=audio 3000 RTP/AVP 0 8 18

a=rtpmap:0 PCMU/8000

a=rtpmap:8 PCMA/8000

a=rtpmap:18 G729/8000

a=silenceSupp:on - - - -

a=crypto:1 AES_CM_128_HMAC_SHA1_80
    inline:cUYqLlpLMDtefkpjW1F4ZjdMS08lMz0sM191RGNQ
```

10.0.1.132	10.0.1.131	SIP/SDP	Request: INVITE sip:200@10.0.1.131:5060;user=phone, with session
10.0.1.131	10.0.1.132	SIP	Status: 401 Unauthorized
10.0.1.132	10.0.1.131	SIP	Request: ACK sip:200@10.0.1.131:5060;user=phone
10.0.1.132	10.0.1.131	SIP/SDP	Request: INVITE sip:200@10.0.1.131:5060;user=phone, with session
10.0.1.131	10.0.1.132	SIP	Status: 100 Trying
10.0.1.131	10.0.1.132	SIP/SDP	Status: 200 OK, with session description
10.0.1.132	10.0.1.131	SIP	Request: ACK sip:200@10.0.1.131:5060
10.0.1.132	10.0.1.131	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x76AC04FE, Seq=7536, Time=288851190
10.0.1.131	10.0.1.132	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x3BA790D3, Seq=51782, Time=288851184,
10.0.1.132	10.0.1.131	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x76AC04FE, Seq=7537, Time=288851350
10.0.1.131	10.0.1.132	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x3BA790D3, Seq=51783, Time=288851344
10.0.1.132	10.0.1.131	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x76AC04FE, Seq=7538, Time=288851510
10.0.1.131	10.0.1.132	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x3BA790D3, Seq=51784, Time=288851504
10.0.1.132	10.0.1.131	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x76AC04FE, Seq=7539, Time=288851670
10.0.1.131	10.0.1.132	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x3BA790D3, Seq=51785, Time=288851664
10.0.1.132	10.0.1.131	SRTP	PT=ITU-T G.711 PCMA, SSRC=0x76AC04FE, Seq=7540, Time=288851830

¿Se me oye?


cap2.pcap - VoIP - RTP Player
5
6
7
8
9
10
11
12
From 10.0.1.132:3000 to 10.0.1.131:13192 Duration:13,70 Drop by Jitter Buff:0(0,0%) Out of Seq: 0(0,0%) Wrong Timestamp: 682(99,9%)
From 10.0.1.131:13192 to 10.0.1.132:3000 Duration:13,81 Drop by Jitter Buff:13(1,9%) Out of Seq: 0(0,0%) Wrong Timestamp: 669(98,0%)
Jitter buffer [ms] 50
Use RTP timestamp
Decode
Play
Pause
Stop
Close

Consideraciones parciales

- Si podemos usarlo, empezamos a usarlo!
- Asterisk 1.8 tiene soporte de TLS y SRTP
- Encriptemos también con la voz con SRTP
- De perdidos al río!
- Si hay una razón para empezar a migrar a 1.8, esta sería casi suficiente

SIP TLS con Asterisk

- Usar una versión de 1.8 (1.8.7.0 @ 03/10/2011)
- Compilar con soporte libsrtp (instalar srtp de sourceforge)
- Configurar debidamente.
- Configurar el terminal , aquí veremos Bria, Aastra 57i , Cisco SPA 525G

SIP TLS con Asterisk (II)

- Revisar que se detecta en ./configure
- TLS no preocuparse. By default

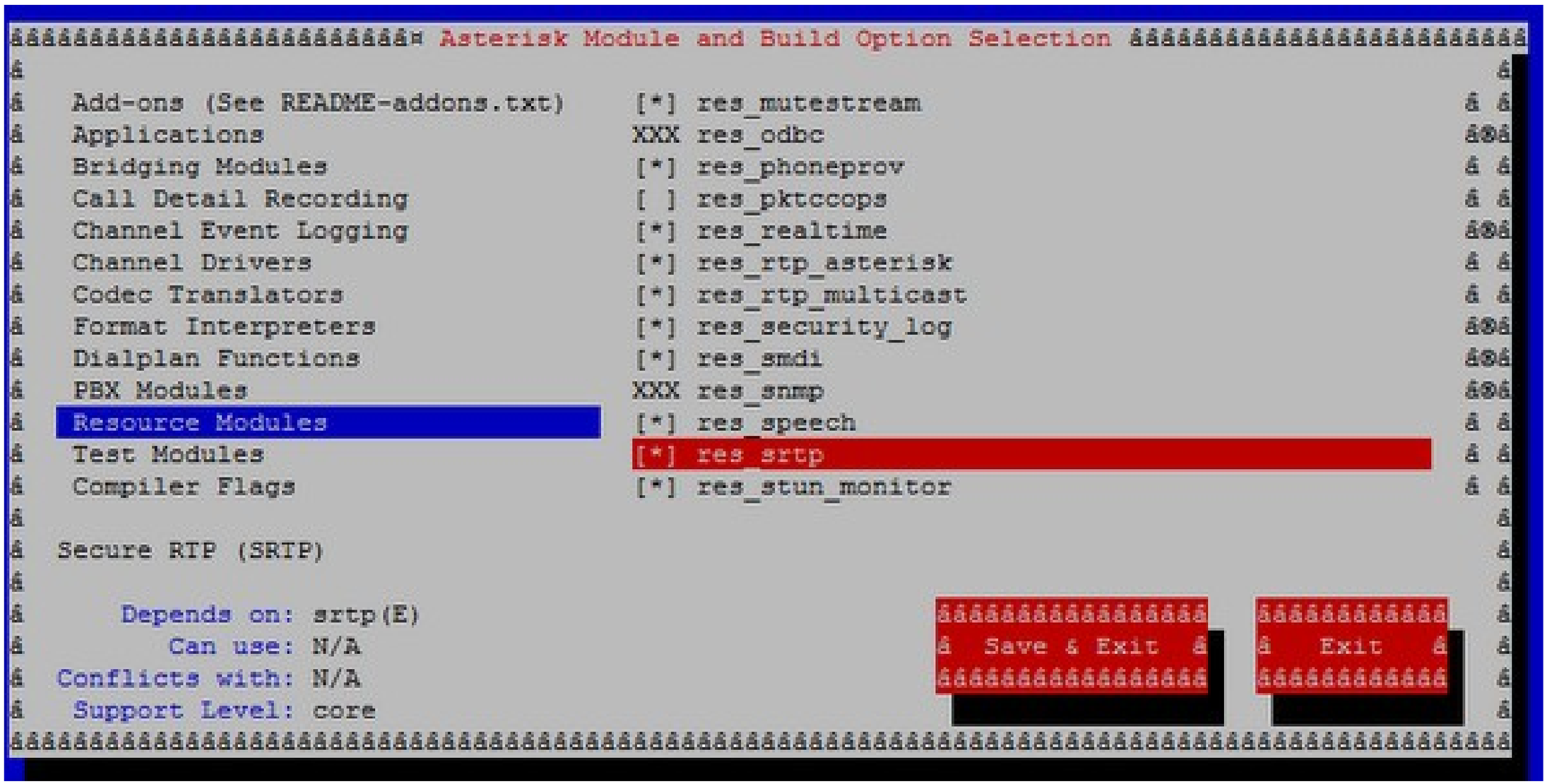
```
checking for srtp_init in -lsrtp... yes

checking srtp/srtp.h usability... yes

checking srtp/srtp.h presence... yes

checking for srtp/srtp.h... yes

checking for the ability of -lsrtp to be linked in a shared
    object... yes
```

SIP TLS con Asterisk (III)

- Y en la compilación nos compila soporte de srtp

```
[CC] sip/dialplan_functions.c -> sip/dialplan_functions.o

   [CC] sip/reqresp_parser.c -> sip/reqresp_parser.o

   [CC] sip/sdp_crypto.c -> sip/sdp_crypto.o

   [CC] sip/srtp.c -> sip/srtp.o

   [LD] chan_sip.o sip/config_parser.o sip/dialplan_functions.o
    sip/reqresp_parser.o sip/sdp_crypto.o sip/srtp.o ->
    chan_sip.so
```

SIP TLS con Asterisk (IIIb)



SIP TLS con Asterisk (IV)

- Sip.conf

```
tlsenable=yes

tlsbindaddr=0.0.0.0

tlscertfile=/etc/asterisk/keys/asterisk.pem

tlscafile=/etc/asterisk/keys/ca.crt

tlscipher=ALL

tlsclientmethod=tlsv1 ;none of the others seem to work with Blink
    as the client
```

SIP TLS con Asterisk (V)

- Sip.conf

```
[101]

type=friend

secret=101

host=dynamic

context=local

dtmfmode=rfc2833

disallow=all

allow=alaw

;transport=tls

context=local

srtpcapable=yes
```

SIP TLS con Asterisk (VI)

- Extensions.conf

```
[local]

exten => _1XX,1,Set(_SIP_SRTP_SDES=optional)

exten => _1XX,n,Dial(SIP/${EXTEN})

exten => _1XX,n,Hangup

exten => 200,1,Set(_SIP_SRTP_SDES=optional)

exten => 200,n,Answer

exten => 200,n,Echo()

exten => 200,n,Hangup
```

Generar Certificados

- Lo más pesado y rebuscado
- En Asterisk 1.8 hay scripts que lo facilitan.
- Mirar en /usr/src/contrib/scripts

Generar Certificados para TLS y *

```
mkdir /etc/asterisk/keys

./ast_tls_cert -C pbx.mycompany.com -O "My Super
   Company" -d /etc/asterisk/keys

./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -
   k /etc/asterisk/keys/ca.key -C phone1.mycompany.com
   -O "My Super Company" -d /etc/asterisk/keys -o
   malcolm
```

```
asterisk.crt asterisk.csr asterisk.key asterisk.pem malcolm.crt
   malcolm.csr malcolm.key malcolm.pem ca.cfg ca.crt ca.key
   tmp.cfg
```

Generar Certificados para TLS y *

Dominios de los certificados

/etc/hosts

```
10.0.1.132 telefono1.voipnovatos.es

10.0.1.106 telefono2.voipnovatos.es

10.0.1.133 telefono3.voipnovatos.es
```

Y para SRTP?

- No necesario generarlos

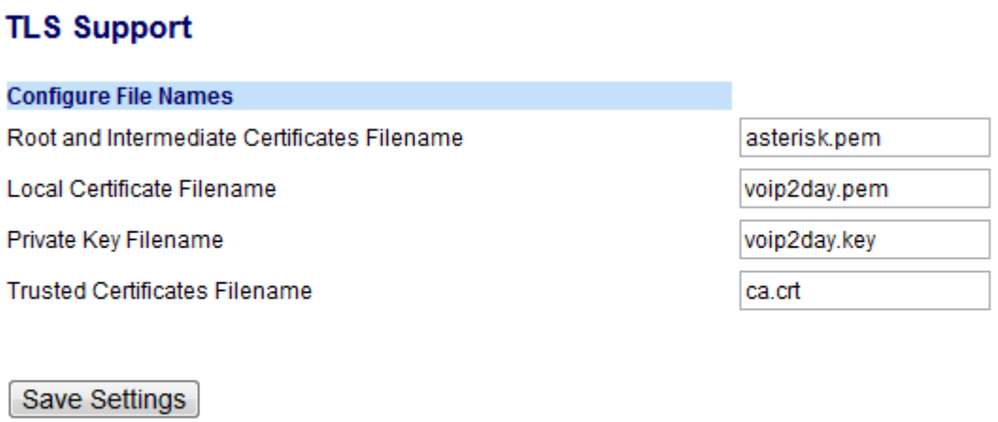
Y ahora los terminales

- Cada fabricante lo pide de una forma
- Aastra pide certificado de PBX, CA, y personal (opcional)
- Cisco simplemente pide activar SIP TLS y SRTP
- Grandstream pide certificado de *, key privada y clave de extension. SRTP varias opciones. Fijado, opcional, no

SIP TLS Aastra 57i st

- En Advanced Options, Global Settings configuraremos TLS

- Y en TLS Support los certificados

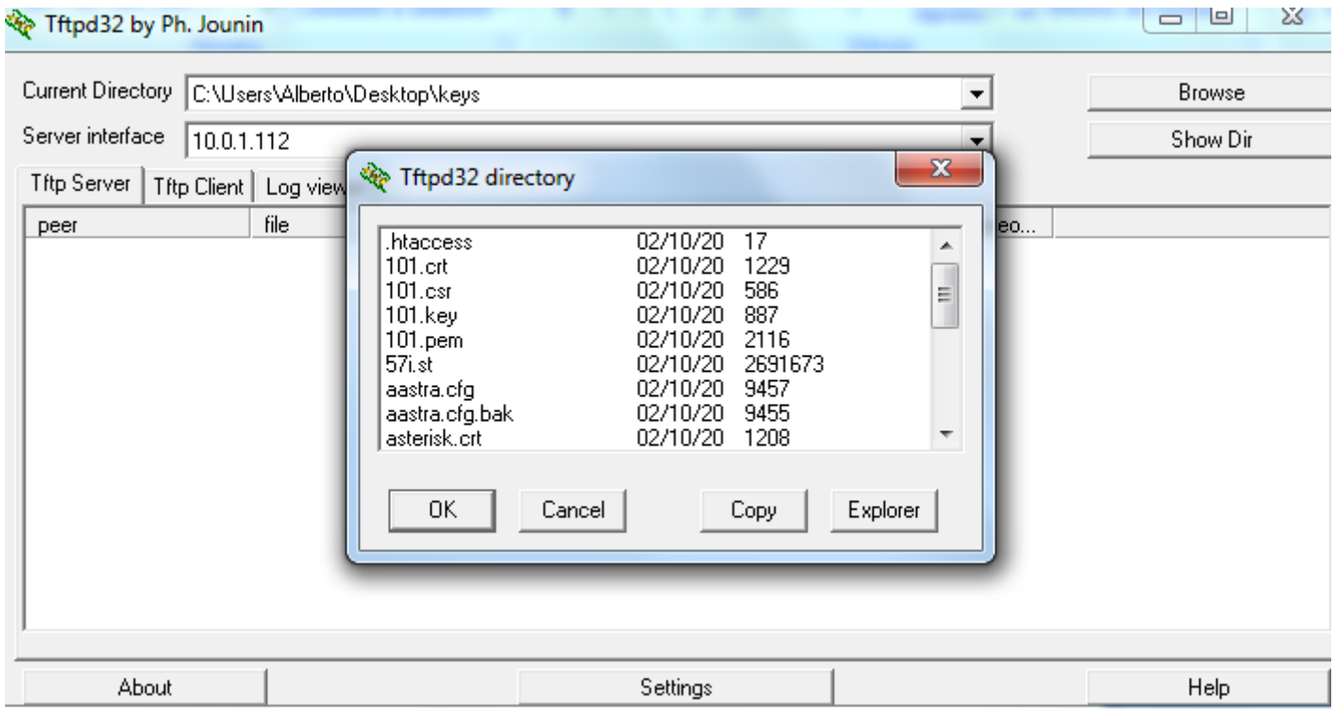


SRTP con Aastra 57i st

- En Advanced Options, Global Settings configuraremos SRTP

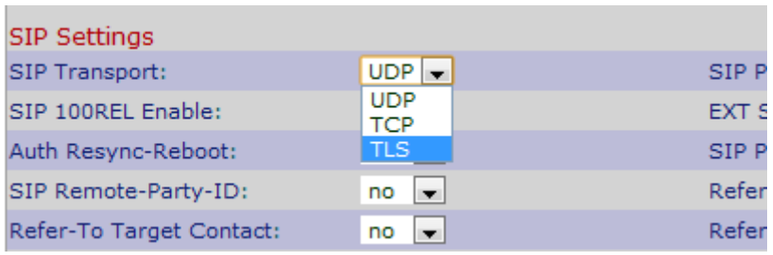
SIP TLS Aastra 57i st

- En aastra los obtiene del TFTP por lo que habrá que poner disponible esos ficheros en el TFTP server así como un aastra.cfg genérico



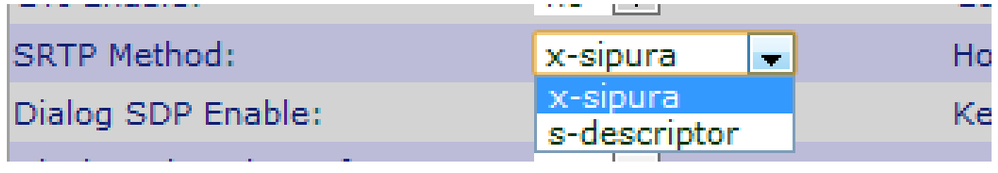
SIP TLS Cisco SPA 525G

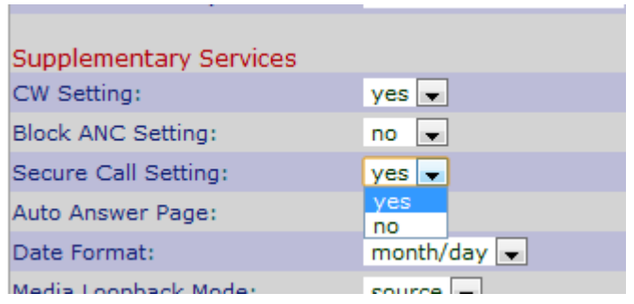
- Se seleccionará SIP TLS en la opción de Transport en la línea correspondiente



- Y para SRTP igualmente en las opciones generales de SIP y USER

a s-descriptor





Llamada entre Aastra y Cisco Con TLS y SRTP

- Problemas encontrados. Sin tocar Asterisk. Llamada de Aastra a Cisco OK. Aastra produce Crash al recibir llamadas y no SRTP porque manda como opcion 32 bits en RTP.

```
a=crypto:1 AES_CM_128_HMAC_SHA1_32
    inline:+5lNkkVkqwSDDnLjXTna+Ut8n901ZlLrU3VtcSYR

a=crypto:2 AES_CM_128_HMAC_SHA1_80
    inline:+5lNkkVkqwSDDnLjXTna+Ut8n901ZlLrU3VtcSYR
```

- Solución : Parchear Asterisk

Llamada entre Aastra y Cisco Con TLS y SRTP

- Parche sencillo

```
int sdp_crypto_offer(struct sdp_crypto *p)

{
        char crypto_buf[128];

//      const char *crypto_suite = "AES_CM_128_HMAC_SHA1_80"; /* Crypto
    offer *

        const char *crypto_suite = "AES_CM_128_HMAC_SHA1_32"; /* Crypto
    offer *



        if (p->a_crypto) {

                ast_free(p->a_crypto);

        }
```

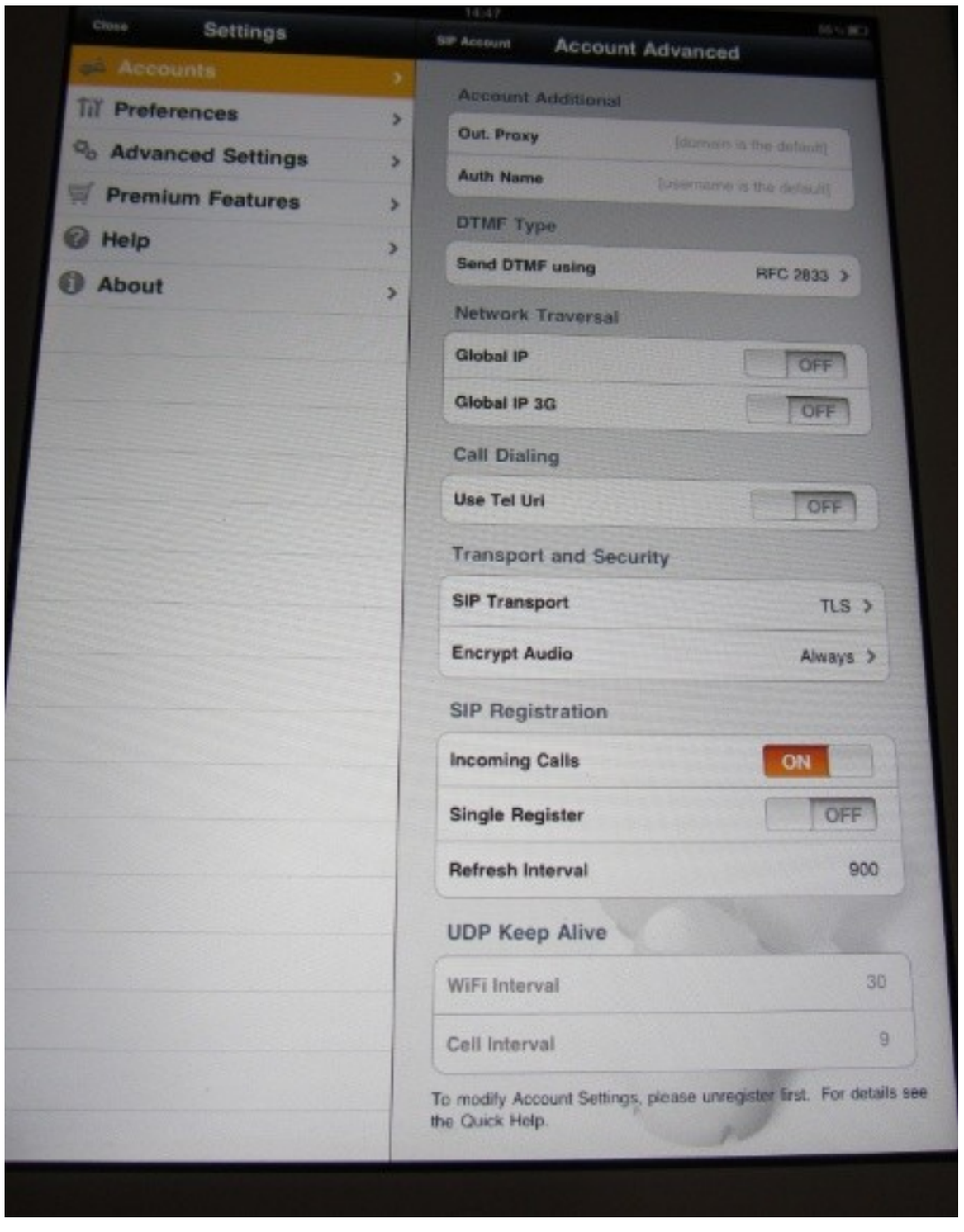
Llamada entre Aastra y Cisco Con TLS y SRTP

- Pero ahora entre Ciscos todo OK. Pero ya no pueden negociar entre distintos fabricantes.
- Readaptar parche a 1.8.7.0
- https://issues.asterisk.org/view.php?id=18674
- Moraleja: Mejorar en compatibilidad entre fabricantes, al menos en SRTP.

Llamada entre Aastra y Cisco Con TLS y SRTP

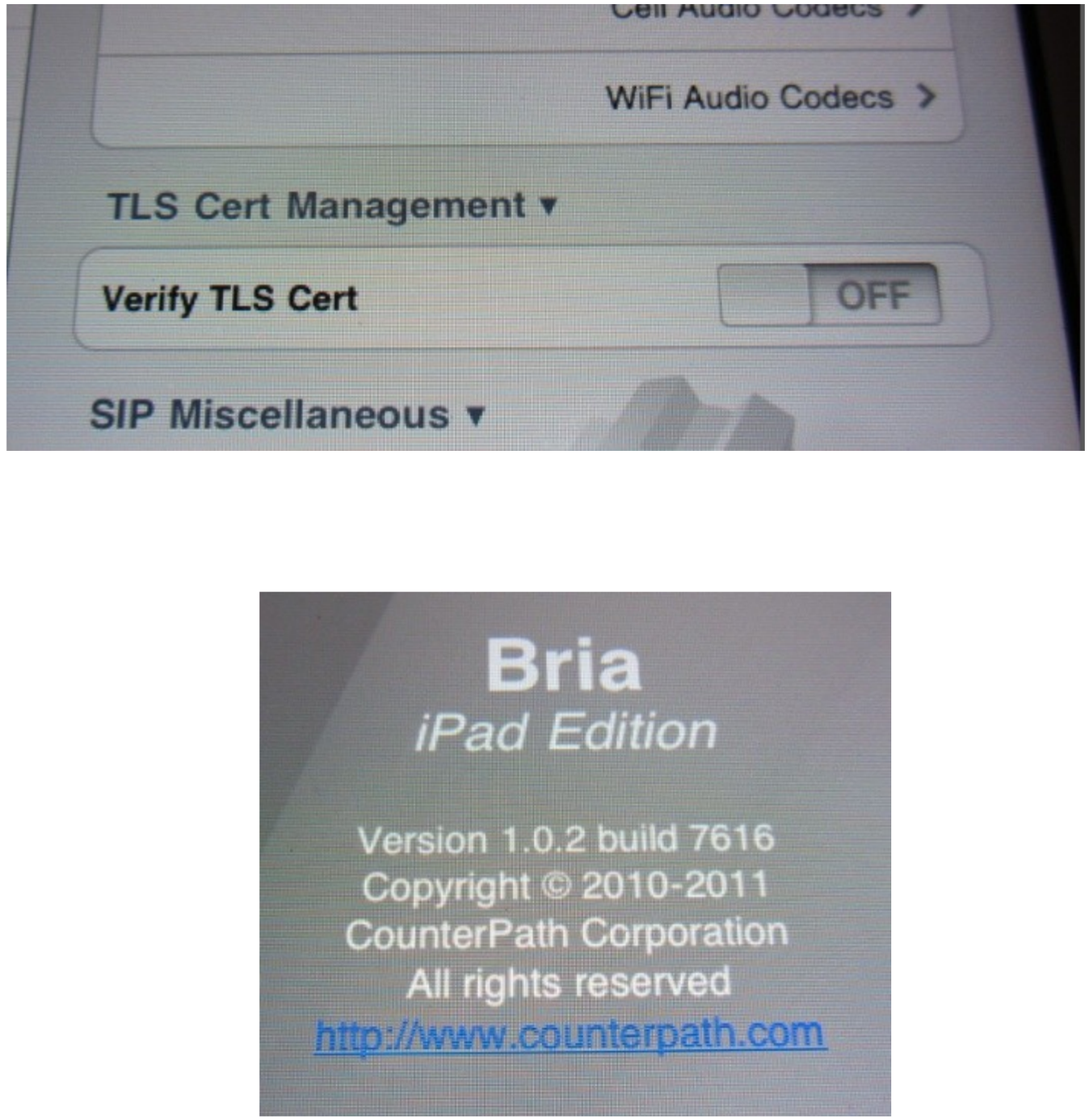
- https://issues.asterisk.org/jira/browse/ASTERISK-17895
- https://issues.asterisk.org/jira/browse/ASTERISK-17895?page=com.atlassian.jira.plugin.ext.subversion%3Asubversion-commits-tabpanel#issue-tabs
- Pasar a Asterisk 10 ☺ ¿Pero si no hemos ni probado 1.8?

SIP TLS & SRTP Bria Ipad

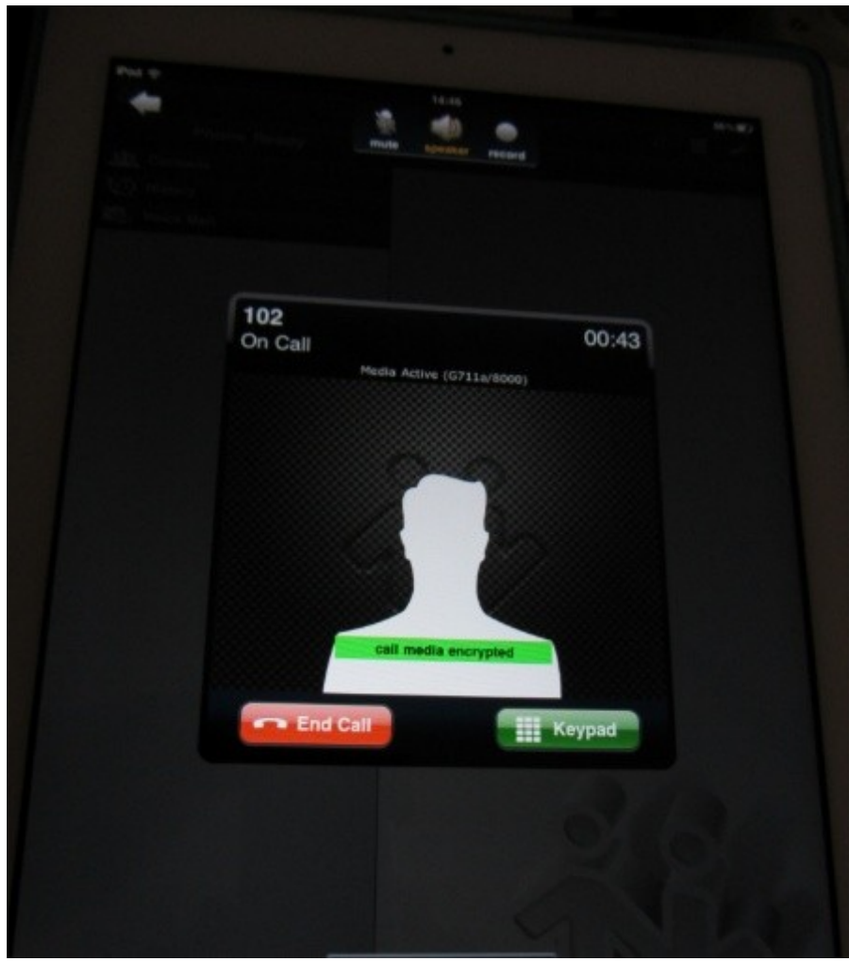


www.voipnovatos.es

SIP TLS & SRTP Bria Ipad



SIP TLS & SRTP Bria Ipad



- Llamadas OK a Cisco , pero no entrantes

Llamada entre Aastra y Bria Ipad

- Crash al recibir llamadas de Ipad
- Pero manda AES_80 y AES_32

SIP TLS & SRTP Acrobits 2.00

www.voipnovatos.es

Llamada entre Aastra / Cisco y Acrobits

- Crash al llamar a Aastra
- No manda SRTP. No tiene soporte
- OK al llamar a Cisco pero no hay audio. Porque no permite SRTP Acrobits.
- Desactivando SRTP TLS OK entre cisco y Acrobits

SIP TLS & SRTP
Grandstream

Configurar certificados TLS y puerto TLS

No funciona a día 03/10/2011 . Notificado a GS

Llamada entre Aastra / Cisco y Grandstream

- Crash al llamar a Aastra
- Traza SRTP OK. Pero no negocia con Asterisk
- OK al llamar a Cisco .
- No se le puede llamar a él. Hay problema con certificados TLS

```
[Oct  3 16:16:33] ERROR[3965]: tcptls.c:176

handle_tcptls_connection: Certificate did not verify: unable to get local issuer certificate

[Oct  3 16:16:33] ERROR[3965]: tcptls.c:202

handle_tcptls_connection: Certificate common name did not match (10.0.1.133)
```

TLS Grandstream OK

- TLS tal que así. Todo OK

Llamada entre Asterisk y Grandstream

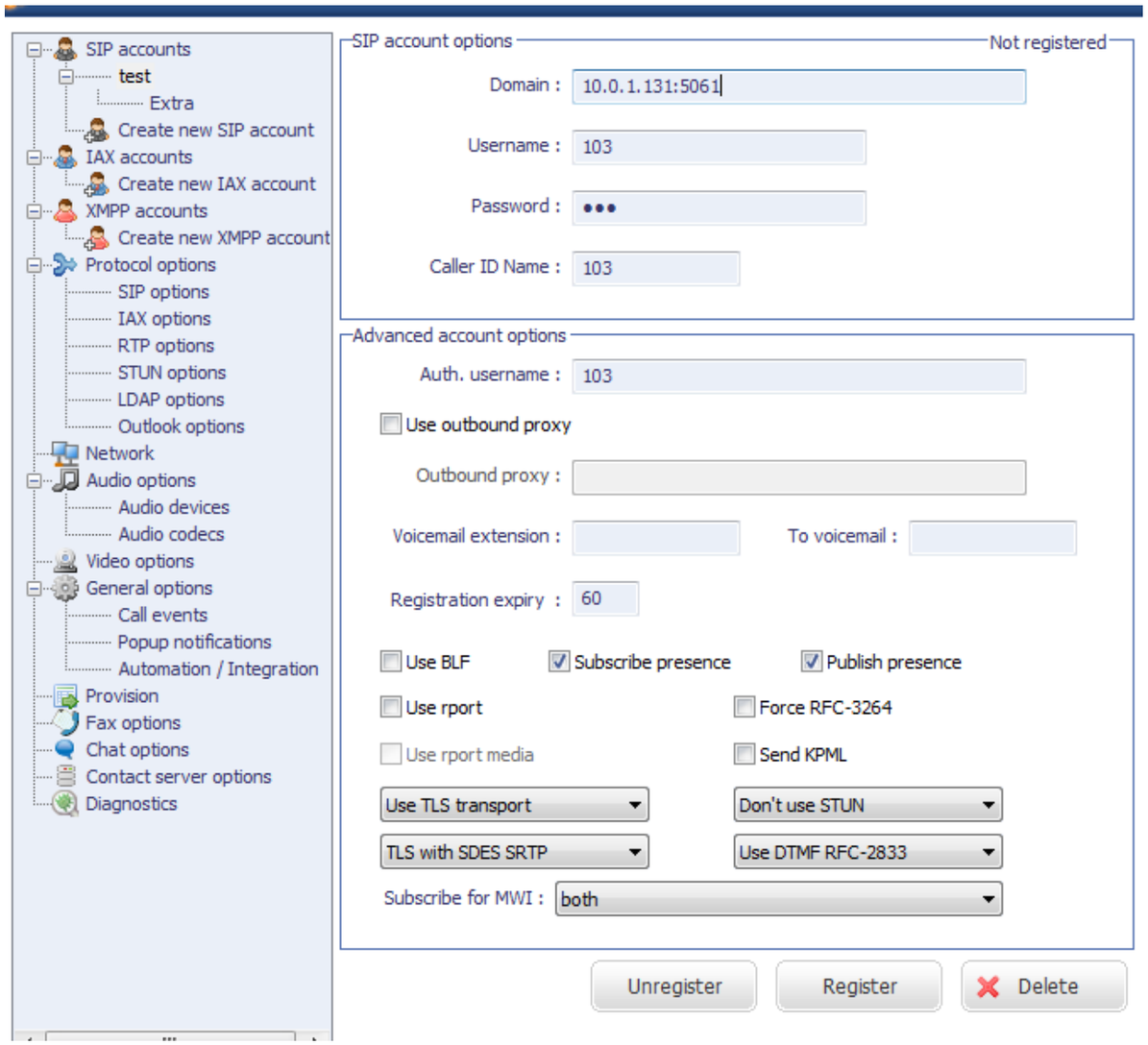
- SRTP con lifetime no soportado

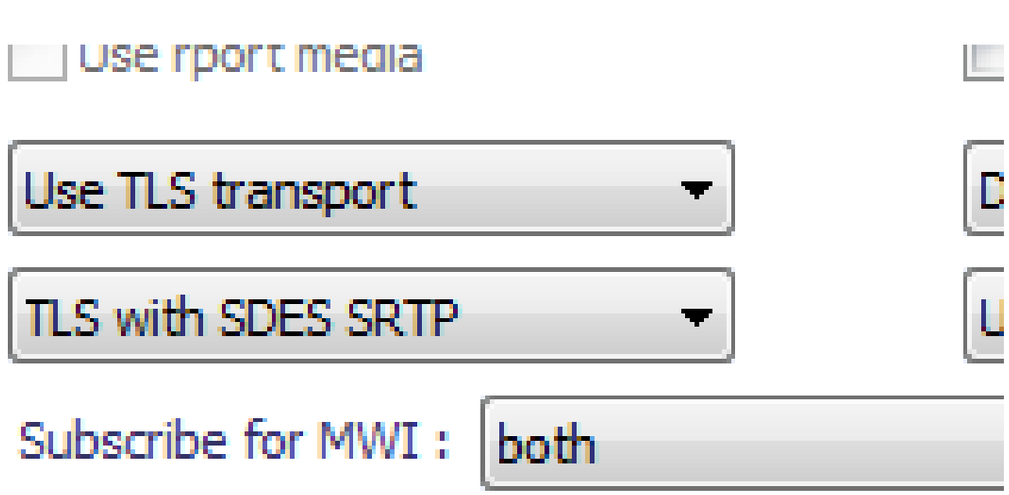
```
[Oct  3 16:43:07] NOTICE[3193]: sip/sdp_crypto.c:250
    sdp_crypto_process: Crypto life time unsupported: crypto:1
    AES_CM_128_HMAC_SHA1_80
    inline:Pzmx5L5pxXG9szCR2UYcEDkBL5SvejE8FZJY/QXv|2^32

[Oct  3 16:43:07] NOTICE[3193]: sip/sdp_crypto.c:260
    sdp_crypto_process: SRTP crypto offer not acceptable

[Oct  3 16:43:07] WARNING[3193]: chan_sip.c:8838 process_sdp:
    Can't provide secure audio requested in SDP offer
```

- Solución : Parche https://issues.asterisk.org/view.php?id=19339

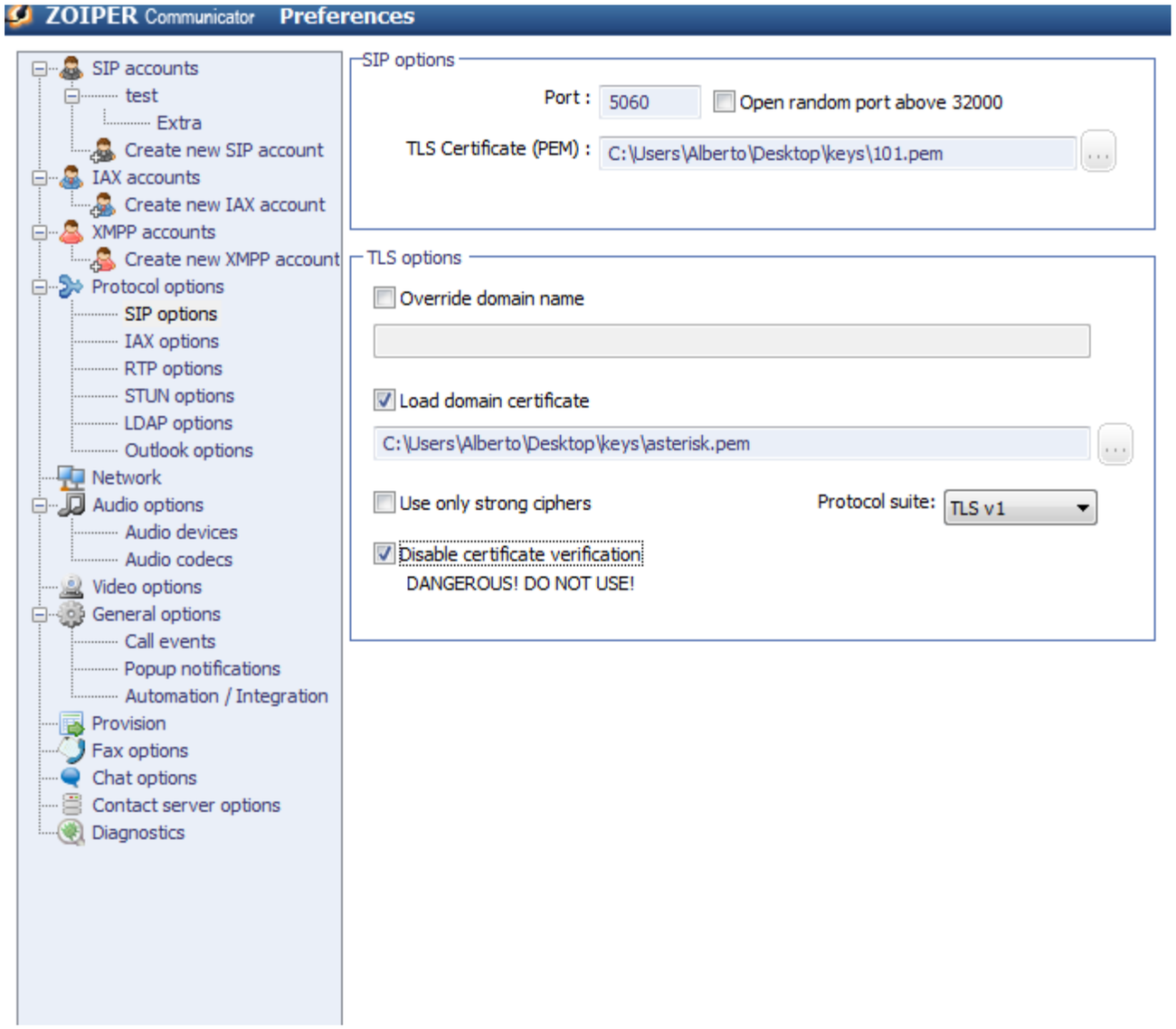
TLS y SRTP con Zoiper Communicator

- Se configura en la pantalla principal.

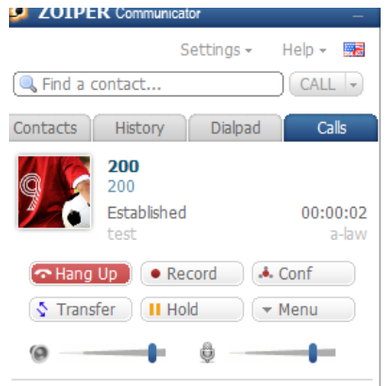




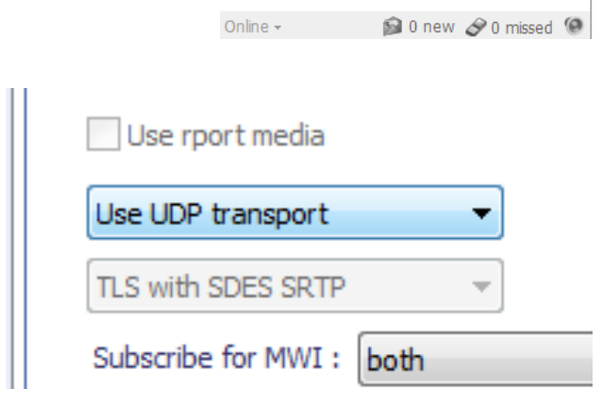
TLS y SRTP con Zoiper Communicator



Llamada entre Asterisk y Zoiper



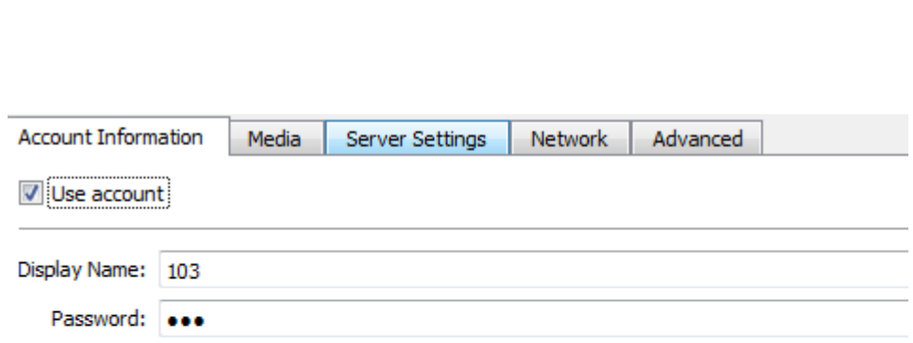
- TLS OK y SRTP OK
- Soporta AES_80
- a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:WpjkRMJa2SxB/MF0MKkdLG5R/VRHWLr7NgD6C7dy

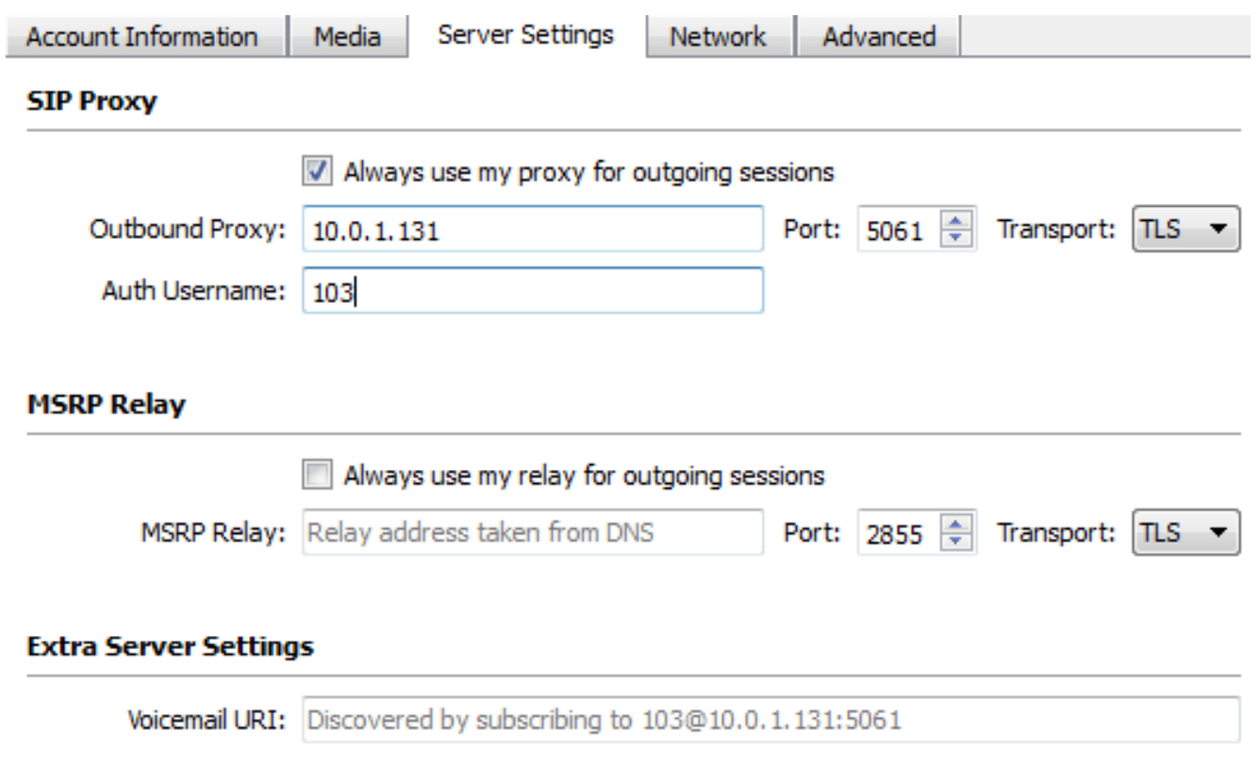


- Si ponemos UDP no deja SRTP
- Si se llama a Aastra crash.
- Si se llama a Cisco OK. Se si le llama error certificados

TLS y SRTP con Blink

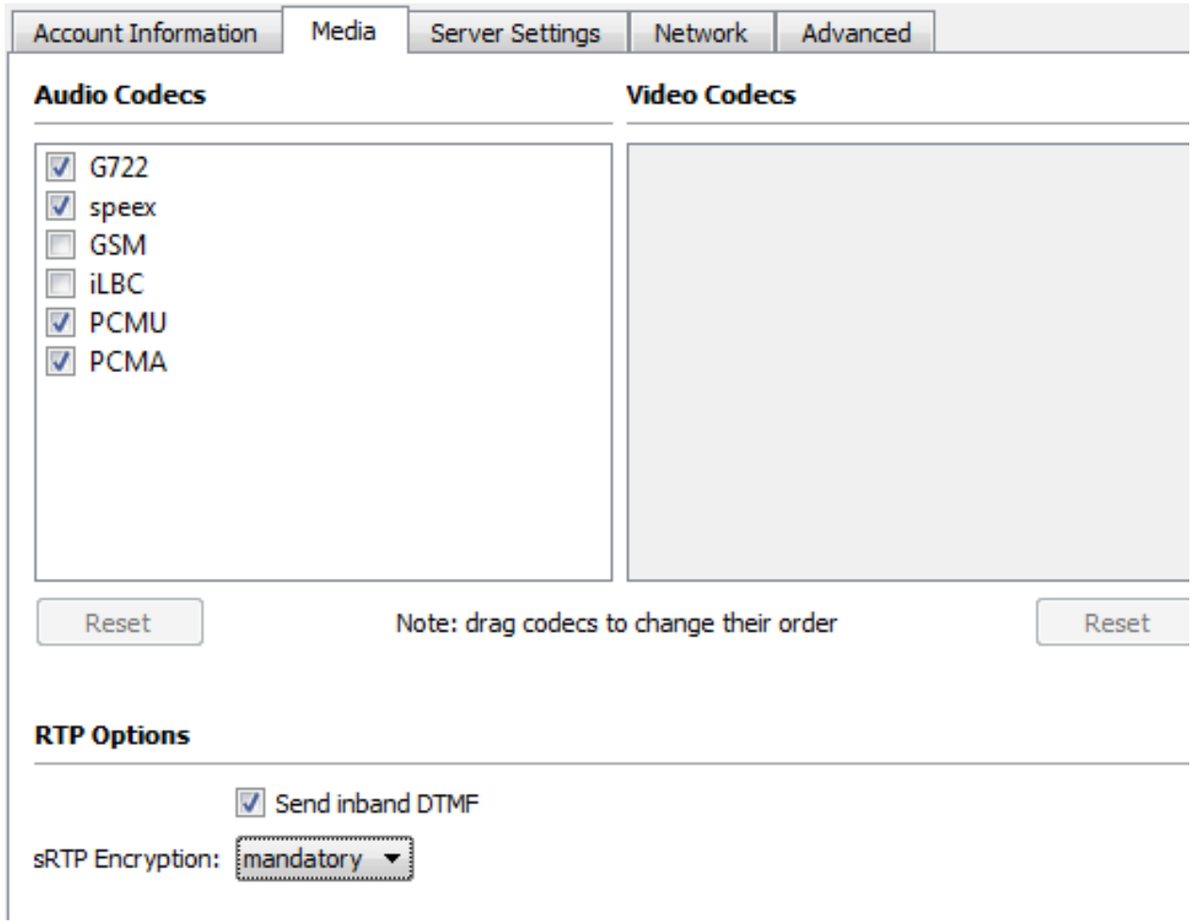
- Se configura en la pantalla principal.

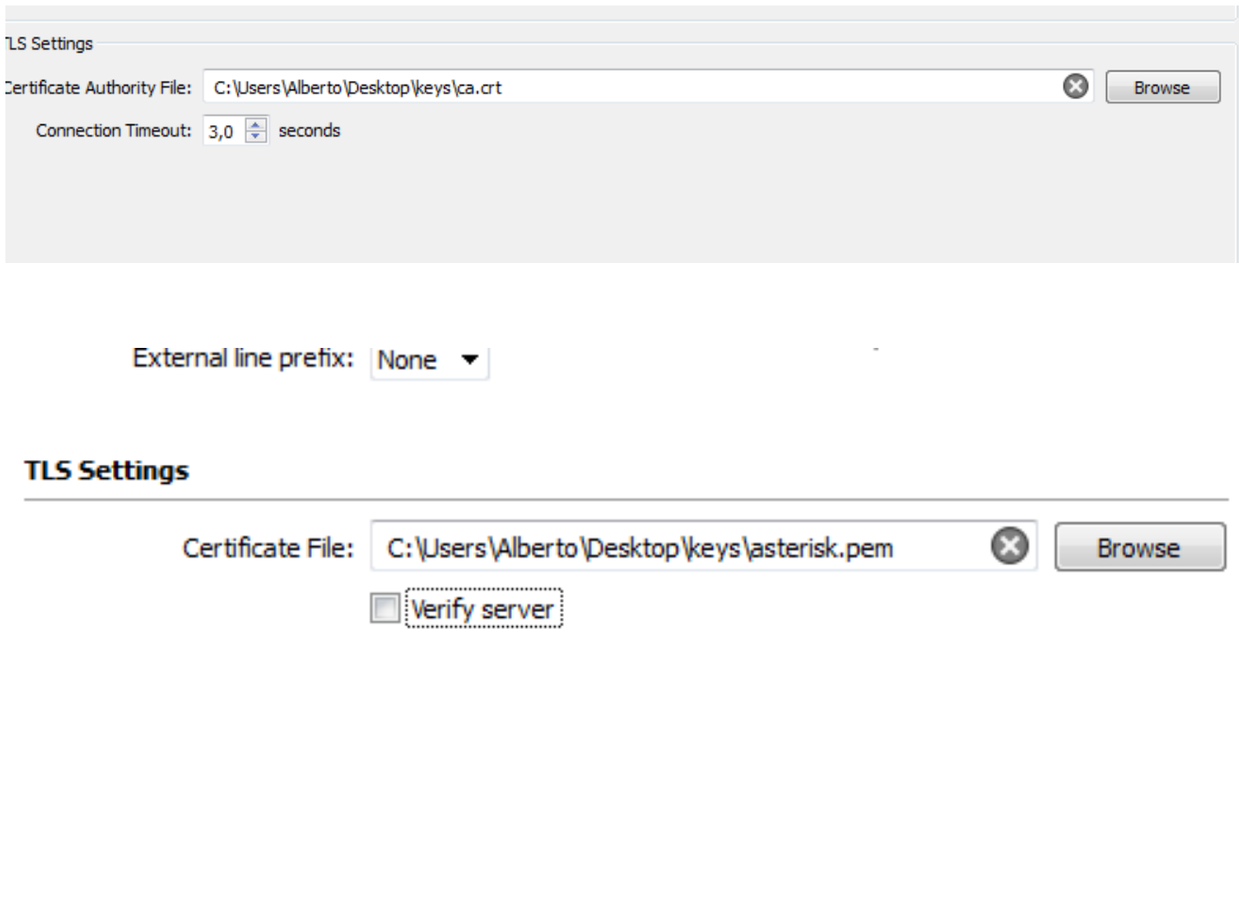




TLS y SRTP con Blink

- Se configura en la pantalla principal.





Llamada entre Asterisk y Blink

- TLS OK y SRTP OK
- Soporta AES_80 y AES_32

- a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:p+Esxwu3zyV/HYScLeDRQI8w1Q67IvP1WT29PoiA
- a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:JiRS0bieTQys730w4exHxTrPmEmDDygR5rP+gjlg

- Llamadas hacia Cisco OK. Desde Cisco ok pero no SRTP . Hay que desactivar SRTP si no 488

Unas Trazas

52 2.926678	10.0.1.132	10.0.1.131	TLSv1	Application Data
53 2.941458	10.0.1.131	10.0.1.132	TCP	sip-tls > dcutility [ACK] Seq=1 Ack=1086 Win=1138 Len=0 TSV=322297 TS
54 2.942658	10.0.1.131	10.0.1.132	TLSv1	Application Data, Application Data
58 2.967772	10.0.1.132	10.0.1.131	TCP	dcutility > sip-tls [ACK] Seq=1086 Ack=571 Win=17376 Len=0 TSV=30556
61 3.008548	10.0.1.132	10.0.1.131	TLSv1	Application Data
64 3.047196	10.0.1.131	10.0.1.132	TCP	sip-tls > dcutility [ACK] Seq=571 Ack=1491 Win=1216 Len=0 TSV=322324
65 3.048387	10.0.1.132	10.0.1.131	TLSv1	Application Data
66 3.048643	10.0.1.131	10.0.1.132	TCP	sip-tls > dcutility [ACK] Seq=571 Ack=2752 Win=1295 Len=0 TSV=322324
67 3.051205	10.0.1.131	10.0.1.132	TLSv1	Application Data, Application Data
75 3.087785	10.0.1.132	10.0.1.131	TCP	dcutility > sip-tls [ACK] Seq=2752 Ack=1133 Win=17376 Len=0 TSV=30568
83 3.144947	10.0.1.131	10.0.1.132	TLSv1	Application Data, Application Data
85 3.147792	10.0.1.132	10.0.1.131	TCP	dcutility > sip-tls [ACK] Seq=2752 Ack=1711 Win=16827 Len=0 TSV=30574
141 5.260661	10.0.1.131	10.0.1.132	TLSv1	Application Data, Application Data
148 5.307951	10.0.1.132	10.0.1.131	TCP	dcutility > sip-tls [ACK] Seq=2752 Ack=2577 Win=17376 Len=0 TSV=30790
150 5.323757	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
152 5.345044	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
154 5.363463	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
155 5.368643	10.0.1.132	10.0.1.131	TLSv1	Application Data
159 5.383419	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
160 5.407247	10.0.1.131	10.0.1.132	TCP	sip-tls > dcutility [ACK] Seq=2577 Ack=3301 Win=1373 Len=0 TSV=322914
164 5.425432	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
166 5.445174	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
168 5.465191	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
170 5.485264	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
171 5.498792	10.0.1.132	10.0.1.131	DIS	Source port: hbci Destination port: 17142
174 5.505189	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
175 5.517423	10.0.1.132	10.0.1.131	DIS	Source port: hbci Destination port: 17142
178 5.525237	10.0.1.131	10.0.1.132	DIS	Source port: 17142 Destination port: hbci
179 5.537166	10.0.1.132	10.0.1.131	DIS	Source port: hbci Destination port: 17142

- ¿Alguien ve algo?
- Los ISP y la espías tampoco.
- TLS/SRTP por 3G! ¿Quien se atreve?

Asterisk CLI TLS

- sip show tcp

```
debian*CLI> sip show tcp

Address                                 Transport    Type

10.0.1.132:1043                         TLS          Server

10.0.1.132:1042                         TLS          Server
```

- sip show channels

```
debian*CLI> sip show channels

Peer              User/ANR         Call ID           Format           Hold
    Last Message    Expiry     Peer

10.0.1.132        101              edbeecf1ee8d49b  0x8 (alaw)        No
    Rx: ACK                    101

1 active SIP dialog
```

Conclusiones

- TLS si es usable hoy en día
- SRTP todavía tienen que madurar un poco en Asterisk
- Fabricantes deben ponerse de acuerdo
- Interoperabilidad casi nula, por no decir nula
- Usarlo más y reportar bugs a asterisk.org. Única vía para mejorarlo

Gracias por vuestra atención

www.voipnovatos.es

Versionado Teléfonos/Softphone

- SPA 525 G v2 7.4.9a
- Aastra 57i 3.2.2.56
- Bria Ipad 1.0.2 build 7616
- Grandstream GXP 2120 1.0.1.83
- Acrobits para Android 2.0
- Zoiper Communicator 2.0.5 11136
- Blink 0.2.7 25 May 2011

“bibliografía”

- https://wiki.asterisk.org/wiki/display/AST/Secure+Calling+Tutorial
- http://voipsa.org/pipermail/voipsec_voipsa.org/2009-March/002938.html
- http://www.remiphilippe.fr/2010/06/04/asterisk-srtp-installation-and-configuration/

“bibliografía”

- http://blog.voz-ip.com/2011/tlssrtp-en-asterisk-1-8/
- tiger.towson.edu/~aalexa3/securingvoiptu.ppt
- https://issues.asterisk.org/view.php?id=18674