



snom Secure VoIP: Call establishment and media protection

Requirements for secure VoIP

- **Protection of SIP-signaling via Secure SIP (SIPS)**
 - Encryption and integrity protection
 - Hop-by-hop
- **Protection of the media**
 - Encryption and integrity protection
 - End-to-end
 - At network (IPSec ESP) or application layer (SRTP)





Secure SIP is similar to HTTPS

- SIPS extends SIP in a similar way as Secure HTTP (HTTPS)
- Secure SIP works like HTTP over TLS (RFC 2818)
- Transport Layer Security (TLS) usage within SIP
- using TLS for UAs is recommended
- TLS cannot be applied to UDP-based SIP signaling





SIP without TLS

- Third-parties are able to trace and intercept your SIP call flows

| No. . | Time | Source | Destination | Protocol | Info |
|-------|-----------|---------------|---------------|----------|----------------------|
| 50 | 5.202126 | 192.168.5.188 | 192.168.0.8 | SIP | Request: NOTIFY sip: |
| 51 | 5.208213 | 192.168.0.8 | 192.168.5.188 | SIP | Status: 200 Ok |
| 214 | 10.088781 | 192.168.5.188 | 192.168.0.8 | SIP/SDP | Request: INVITE sip: |
| 215 | 10.090279 | 192.168.5.188 | 192.168.0.8 | SIP | Request: NOTIFY sip: |
| 216 | 10.097101 | 192.168.0.8 | 192.168.5.188 | SIP | Status: 100 Trying |


```
▶ Session Initiation Protocol
▼ Session Initiation Protocol (SIP as raw text)
  INVITE sip:01621036822@intern.snom.de;user=phone SIP/2.0\r\n
  Via: SIP/2.0/UDP 192.168.5.188:5060;branch=z9hG4bK-dkff6vd90lo6;rport\r\n
  From: "411" <sip:411@intern.snom.de>;tag=j3tkpeu52j\r\n
  To: <sip:01621036822@intern.snom.de;user=phone>\r\n
  Call-ID: 53bc99435cbe-7798ubi2wxjl@snom360-00041323021D\r\n
  CSeq: 1 INVITE\r\n
  Max-Forwards: 70\r\n
  Contact: <sip:411@192.168.5.188:5060;line=6gxpc688>;flow-id=1\r\n
  P-Key-Flags: resolution="31x13", keys="4"\r\n
  User-Agent: snom360\r\n
```



Using Secure SIP in snom phones

- Add these parameters into the Outbound Proxy-Field:

intern.snom.de:5061;transport=tls

- Port 5061 is the standard Secure SIP port and works with TCP

- If the provider sets a SIPS DNS SRV record, the Outbound Proxy-Field is not needed.

| Login | SIP | NAT | RTP |
|---------------------------|---|-----|-----|
| Login Information: | | | |
| Line active: | <input checked="" type="radio"/> on <input type="radio"/> off | | |
| Displayname: | 211 | | |
| Account: | 211 | | |
| Password: | *** | | |
| Registrar: | intern.snom.de | | |
| Outbound Proxy: | intern.snom.de:5061;transport=tls | | |
| Authentication Username: | | | |

Sent to tls:192.168.0.8:5061 at 17/2/2006 14:17:31:890 (804 bytes):

```
REGISTER sip:intern.snom.de SIP/2.0
Via: SIP/2.0/TLS 192.168.6.190:2129;branch=z9hG4bK-6mmhw9iqbr0;rport
From: "211" <sip:211@intern.snom.de>;tag=ggsmo5poc
To: "211" <sip:211@intern.snom.de>
Call-ID: 3c267766d6d8-18qi46kp2f63@snom360-000413231517
CSeq: 16 REGISTER
Max-Forwards: 70
Contact:
<sip:211@192.168.6.190:2129;transport=tls;line=wxgyax8>;flow-id=1;q=1.0;+sip.instance
User-Agent: snom360/5.3
Allow-Events: dialog
X-Real-IP: 192.168.6.190
WWW-Contact: <http://192.168.6.190:80>
WWW-Contact: <https://192.168.6.190:443>
Expires: 3600
Content-Length: 0
```

Received from tls:192.168.0.8:5061 at 17/2/2006 14:17:32:050 (602 bytes):

```
SIP/2.0 200 Ok
Via: SIP/2.0/TLS 192.168.6.190:2129;branch=z9hG4bK-k2uh2iwba3ha;rport=2129
From: "211" <sip:211@intern.snom.de>;tag=r419q96sdn
To: "211" <sip:211@intern.snom.de>;tag=1634
Call-ID: 3c26700a0753-j20zfrid9hj9@snom360-000413231517
CSeq: 15 REGISTER
```




Tracing protected SIP messages

- There is no opportunity for third-parties to intercept your SIP messages
- The TLS communication between your snom phone and the registrar is now safe

| No. . | Time | Source | Destination | Protocol | Info |
|-------|----------|---------------|---------------|----------|-------------------|
| 18 | 3.644615 | 192.168.6.190 | 192.168.0.8 | TLS | Application Data |
| 20 | 3.652312 | 192.168.0.8 | 192.168.6.190 | TLS | Application Data |
| 25 | 3.699558 | 192.168.6.190 | 192.168.0.8 | TLS | Application Data, |
| 27 | 3.700251 | 192.168.6.190 | 192.168.0.8 | TLS | Application Data |
| 29 | 3.711469 | 192.168.0.8 | 192.168.6.190 | TLS | Application Data |
| 31 | 3.719555 | 192.168.0.8 | 192.168.6.190 | TLS | Application Data |
| 33 | 3.731943 | 192.168.0.8 | 192.168.6.190 | TLS | Application Data |
| 37 | 3.751962 | 192.168.6.190 | 192.168.0.8 | TLS | Application Data |
| 39 | 3.760410 | 192.168.0.8 | 192.168.6.190 | TLS | Application Data |
| 41 | 3.805707 | 192.168.6.190 | 192.168.0.8 | TLS | Application Data, |
| 45 | 3.806569 | 192.168.6.190 | 192.168.0.8 | TLS | Application Data |
| 48 | 3.826430 | 192.168.0.8 | 192.168.6.190 | TLS | Application Data |
| 55 | 3.885313 | 192.168.6.190 | 192.168.0.8 | TLS | Application Data |

Frame 18 (226 bytes on wire, 226 bytes captured)

```
0000 00 06 7b 01 b4 43 00 04 13 23 15 17 08 00 45 00  ..{..C.. .#....E.
0010 00 d4 ce c6 40 00 40 06 e3 46 c0 a8 06 be c0 a8  ....@.@. .F.....
```

Certificate management Service for SIP

- certificates by SIP servers are very similar to those used by web servers
- a given domain, example.com, will get one certificate for each server to route interdomain SIP requests
- UAs registering or being challenged can also view this certificate to ensure that they are connected to a valid server (not a server spoofing the domain)
- certificates can be identical to the standard e-commerce certificates supported today by web browsers
- possible that UA could have e-commerce cert, that is not a scalable approach for millions of UAs

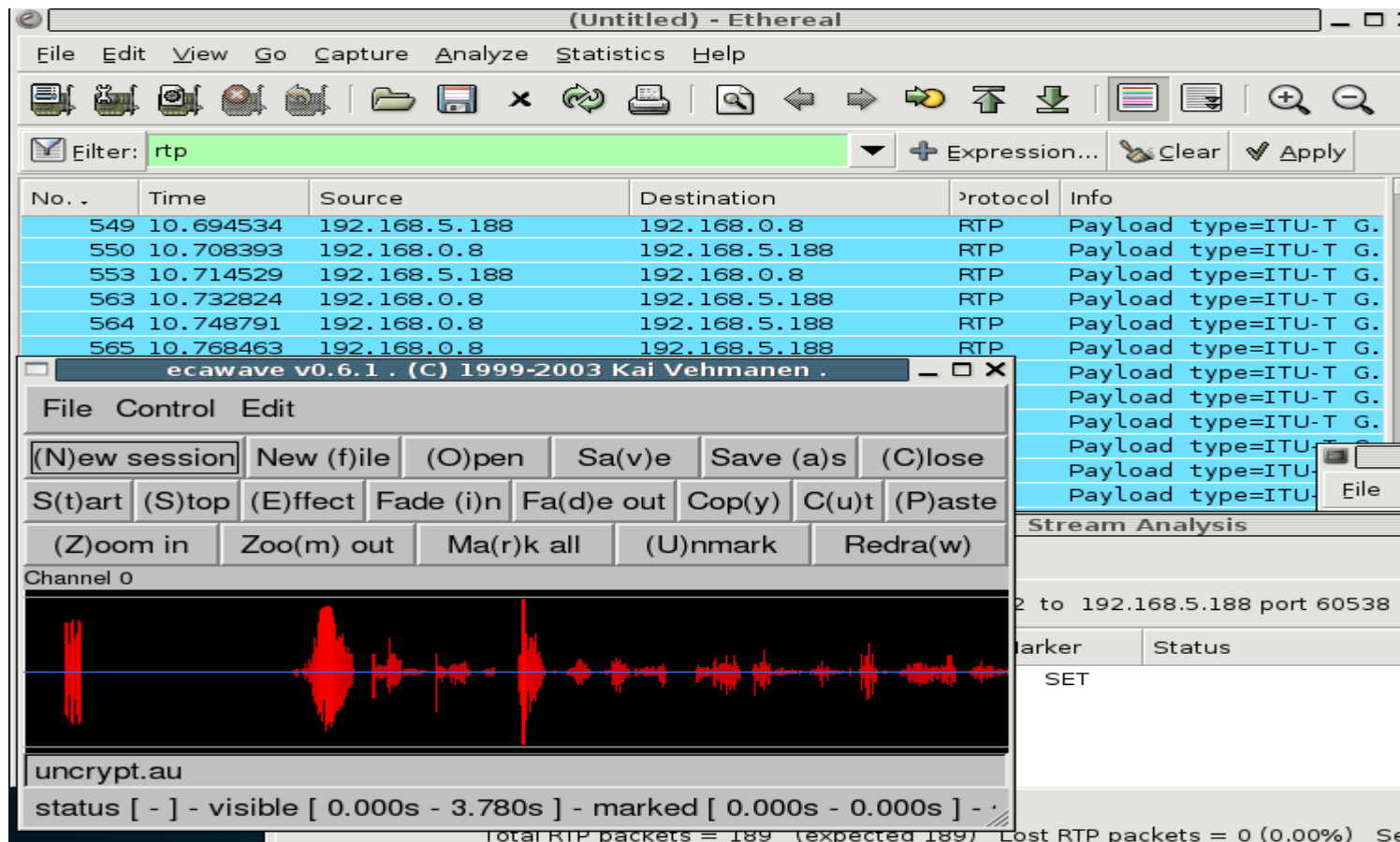
Secure RTP (SRTP)

- ciphared RTP payload
- ciphering in snom phones via Advanced Encryption Standard (AES)
- using AES 128 bit also known as Rijndael
- AES was adopted by National Institute of Standards and Technology (NIST) as US FIPS PUB 197 in November 2001
- sdescriptions describes a way of establishing security parameters for SRTP with SDP attribute a=crypto
- attribute is not a key management protocol like Multimedia Internet KEYing (MIKEY)
- the transmission of the key makes only sense in combination with TLS



Unsecure RTP

- It is the same like in unsecure SIP, third-parties can intercept your media streams




The screenshot shows a Wireshark capture of RTP traffic. The main pane displays a list of captured packets with the following data:

| No. . | Time | Source | Destination | Protocol | Info |
|-------|-----------|---------------|---------------|----------|-----------------------|
| 549 | 10.694534 | 192.168.5.188 | 192.168.0.8 | RTP | Payload type=ITU-T G. |
| 550 | 10.708393 | 192.168.0.8 | 192.168.5.188 | RTP | Payload type=ITU-T G. |
| 553 | 10.714529 | 192.168.5.188 | 192.168.0.8 | RTP | Payload type=ITU-T G. |
| 563 | 10.732824 | 192.168.0.8 | 192.168.5.188 | RTP | Payload type=ITU-T G. |
| 564 | 10.748791 | 192.168.0.8 | 192.168.5.188 | RTP | Payload type=ITU-T G. |
| 565 | 10.768463 | 192.168.0.8 | 192.168.5.188 | RTP | Payload type=ITU-T G. |

Below the packet list, a packet details pane shows the selected RTP packet structure, including 'Stream Analysis' and 'Channel 0'. At the bottom, an audio waveform is displayed, showing the captured audio data. The status bar at the bottom indicates 'Total RTP packets = 189 (expected 189) Lost RTP packets = 0 (0.00%)'.

Activating secure RTP in snom phones

- Enable in the Configuration Line under the RTP menu “RTP Encryption”



[Login](#) [SIP](#) [NAT](#) [RTP](#)

RTP Line Settings:

| | |
|------------------|---|
| Codec 1: | G.711u |
| Codec 2: | G.711a |
| Codec 3: | G.722 |
| Codec 4: | G.726-32 |
| Codec 5: | GSM FR |
| Codec 6: | G.729A |
| Codec 7: | G.723.1 |
| Packet Size: | 20 ms |
| Symmetrical RTP: | <input type="radio"/> on <input checked="" type="radio"/> off |
| RTP Encryption: | <input checked="" type="radio"/> on <input type="radio"/> off |

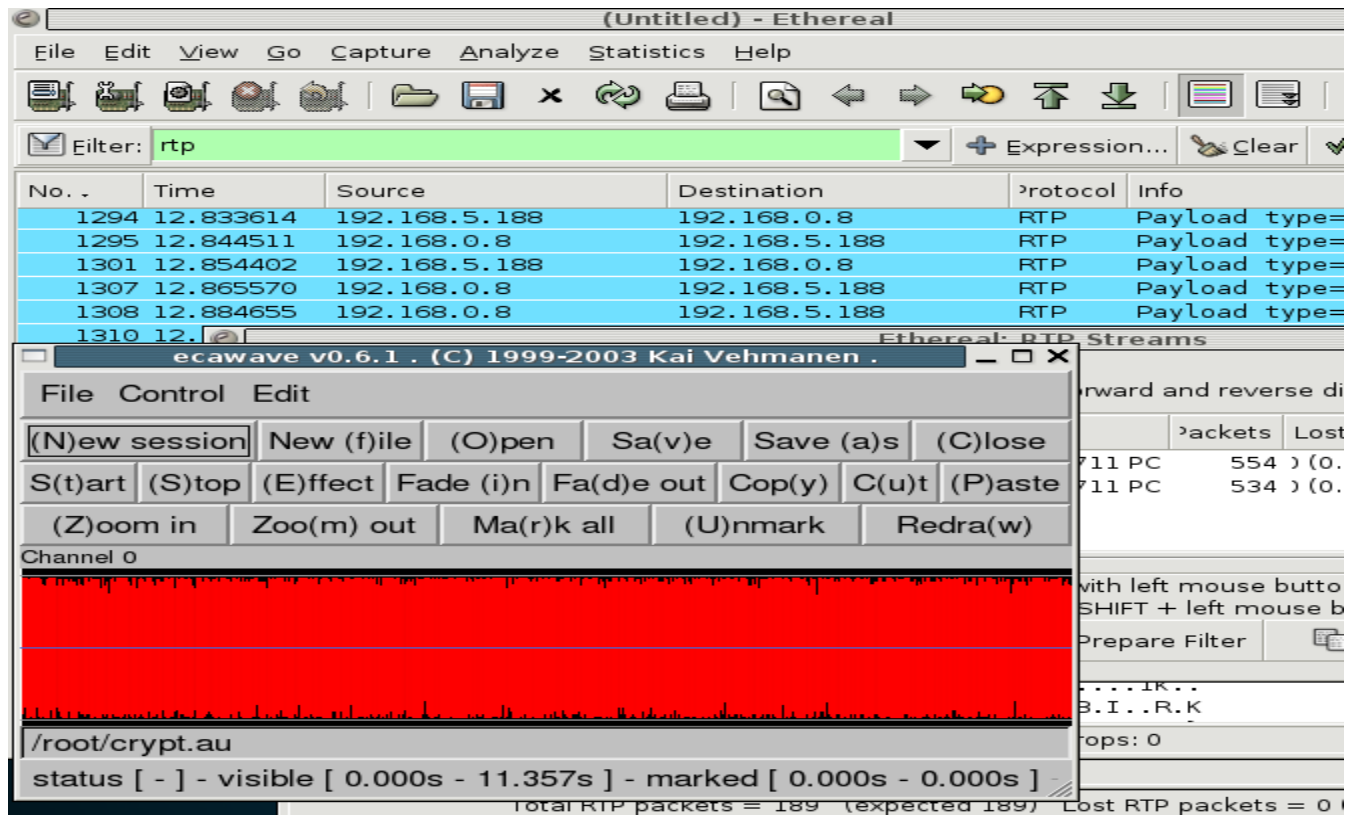
What will happen

- A crypto key will be delivered by SDP. If you are using unsecure SIP the key will be delivered in clear text.

```
Authorization: Digest username="411",realm="intern.snom.de",nonce="6fcc3959fa77e20602e12
Content-Type: application/sdp\r\n
Content-Length: 477\r\n
\r\n
v=0\r\n
o=root 1433039877 1433039877 IN IP4 192.168.5.188\r\n
s=call\r\n
c=IN IP4 192.168.5.188\r\n
t=0 0\r\n
m=audio 53920 RTP/AVP 0 8 9 2 3 18 4 101\r\n
a=crypto:1 AES_CM_128_HMAC_SHA1_32 inline:jIq5uMZ262ZEPprnKjijtOK5h+PwahwiEtecu14h\r\n
a=rtpmap:0 pcmu/8000\r\n
a=rtpmap:8 pcma/8000\r\n
```

Ciphered RTP

- If your crypto key is transported via TLS, third-parties have no chance to decrypt the ciphered RTPs



The screenshot shows the Wireshark interface with a filter set to 'rtp'. The packet list pane displays several RTP packets. The packet details pane shows the 'Ethereal: RTP Streams' section, which includes a spectrogram of the audio data. The spectrogram shows a red waveform, indicating that the audio is encrypted (ciphered).

| No. . | Time | Source | Destination | Protocol | Info |
|-------|-----------|---------------|---------------|----------|---------------|
| 1294 | 12.833614 | 192.168.5.188 | 192.168.0.8 | RTP | Payload type= |
| 1295 | 12.844511 | 192.168.0.8 | 192.168.5.188 | RTP | Payload type= |
| 1301 | 12.854402 | 192.168.5.188 | 192.168.0.8 | RTP | Payload type= |
| 1307 | 12.865570 | 192.168.0.8 | 192.168.5.188 | RTP | Payload type= |
| 1308 | 12.884655 | 192.168.0.8 | 192.168.5.188 | RTP | Payload type= |
| 1310 | 12.895541 | 192.168.0.8 | 192.168.5.188 | RTP | Payload type= |



Conclusion

- **snom phones implement**
 - ciphered RTP payload
 - Secure SIP
 - snom phones guarantee Secure VoIP environment

