How to decode SIP over TLS with Wireshark

For security reasons, some customers may choose to use TLS for the SIP transport. TLS encrypts the SIP signaling messages, but a packet capture will not reveal their content. To troubleshoot this, the signaling messages must be decrypted.

Step-by-step guide

Take the capture

The first step is to capture the call. The call can have legs over TLS, UDP or TCP. Also, the ports can be 5060 or 5061 for Kamailio or 5050 for Asterisk.

1. To capture all of them, run the following command:

| | tcpdump -r | nni any - | s O por | t 5050 or | port 5060 or | port 5 | 061 -w /u | sr/local/voipr | now/admin/htdocs/tls.pcap |
|------|---------------------------------|---|------------------------|-------------------------------|-------------------------------|----------------------------|--------------------------------------|---|--|
| 2. \ | When you ope | n the captu | re, you'll s | ee that the T | LS part of the ca | III is not ev | en recognize | ed by Wireshark as | s SIP. |
| | in the capture | L(C) on LID | D of 102 1 | 10000 priorie (| erminal (A) 192. | o part boty | Inrough the | Volpinow server (B | b) at 10.150.20.27 and towards another |
| 1 | communication | n between F | B and C or | ccurs on UDF | and is visible. In | e part betw | ire, the enco | ded packets will a | ppear as TI S |
| | | 4 + + 0 7 <u>4</u> [| | | | | | | |
| F | ilter | Expression Clear Apply Save | | | tis.pcap - Graph Analysis | | | | |
| k | p. Time | Source | Protocol | Destination | Length Info | | | | |
| | 1 2015-05-26 15:06:29.701 | 1869 192.168.1.225 | TLSV1 | 10.150.20.27 | 1069 Application Data | Time | 10.150.20.27 | Comment | |
| | 2 2015-05-26 15:06:29.712 | 2115 10.150.20.27 | TLSVI | 192.168.1.225 | 391 Application bata | | LJELOOIJEJE | common | |
| | 3 2013-05-26 15:08:29.713 | 192.108.1.225 | CTD (CDD | 10.150.20.27 | 08 45108 > Sips [ACK] Sedel | 2015-05-26 15:06:29.757904 | rwite sug (graz gritt) gritte grav | SIP From: "extA" <sip:00091001@1015020.275061 th="" to:<sip:0<=""><th></th></sip:00091001@1015020.275061> | |
| | 5 2015-05-26 15:06:29 762 | 2930 10 150 20 27 | STP | 10.150.20.27 | 753 Status: 100 Trying | 2015-05-26 15:06:29.762930 | 100 Taying | SIP Status | |
| | 6 2015-05-26 15:06:29,826 | 532 10.150.20.27 | STP/SDP | 10, 150, 20, 27 | 2487 Request: INVITE sin:0001 | 2015-05-26 15:06:29 826532 | INVITE 508 (9711A opus 67221 67221 | SIP From: "Default user" <sip.001@10.150.20.27.5050 th="" to:<sip<=""><th></th></sip.001@10.150.20.27.5050> | |
| | 7 2015-05-26 15:06:29,830 | 784 10.150.20.27 | SIP | 10,150,20,27 | 375 Status: 100 trying ve | 2015-05-26 15:06:29 830784 | 100 trying your call is important to | SIP Status | |
| | 8 2015-05-26 15:06:29.830 | 10.150.20.27 | IPv4 | 192.168.3.152 | 1516 Fragmented IP protocol (| 2015/05/26 15:05:29 891351 | 180 Ringing | OP Status | |
| | 9 2015-05-26 15:06:29.891 | 1351 192.168.3.152 | SIP | 10.150.20.27 | 560 Status: 180 Ringing | 2015 05 26 15 06 20 001260 | 180 Engine | CD Dates | |
| | 10 2015-05-26 15:06:29.892 | 2769 10.150.20.27 | SIP | 10.150.20.27 | 529 status: 180 Ringing | 2015-05-20 1500029 892709 | 100 0000 | SP SHEE | |
| | 11 2015-05-26 15:06:29.893 | 3959 10.150.20.27 | SIP | 10.150.20.27 | 769 Status: 180 Ringing | 2015-05-26 15:06:29.893959 | Tan Kiddiud | S2P Status | |
| | 12 2015-05-26 15:06:29.895 | 5457 10.150.20.27 | TL5V1 | 192.168.1.225 | 691 Application Data | 2015-05-26 15:06:33:699724 | 200 OK SEP (g711A GSM g711U spees | SIP Status | |
| | 13 2015-05-26 15:06:29.896 | 5328 192.168.1.225 | TCP | 10.150.20.27 | 68 43108 > sips [ACK] Seq=1 | 2015-05-26 15:06:33.701654 | 200 OK SEP (g711A GSM g711U spee | SP Satus | |
| | 14 2015-05-26 15:06:33.699 | 9724 192.168.3.152 | SIP/SDP | 10.150.20.27 | 1099 Status: 200 OK | 2015-05-26 15:06:33:703136 | ACK | SIP Request | |
| | 15 2015-05-26 15:06:33.701 | 10.150.20.27 | SIP/SDP | 10.150.20.27 | 1068 Status: 200 OK | 2015/05/26 15:06:33 204540 | ACK | 122 Remark | |
| | 16 2015-05-26 15:06:33.703 | 3136 10.150.20.27 | SIP | 10.150.20.27 | S42 Request: ACK S1p:0003*00 | 2011 01 21 10 01 01 00 000 | 200 OK SPR (a7114 a7111) telephone | (1) (mm) | |
| | 17 2015-05-26 15:08:33.704 | 10.150.20.27 | 51P | 192.108.3.152 | SUB Request: ACK STP:0003-00 | 2013/03/20 13:00:33 303462 | 0003/0802 | SP Maus | |
| | 18 2013-03-20 13:00:33:909 | 10.130.20.27 | DIF/DUP | 10.130.20.27 | 1448 Status, 200 0K 1 | 2015-05-26 15:06:34 086535 | 000,000 | SIP Request | |
| | Course 1, 1050 hotes on other (| (SEE2 bits) 2000 buters | antoned (SEE) bits) | | | 2015-05-26 15:06:39.048094 | 6693,6693 | SIP Request | |
| | I down cooked conture | (8552 DTCS), 1009 byces (| aptured (8332 bits) | | | 2015-05-26 15:06:39.048751 | 201.QK | SIP Status | |
| 5 | Internet Protocol Version 4. | Sec: 192, 168, 1, 225 (192, | 168.1.225), DST: 10.1 | 150, 20, 27 (10, 150, 20, 27) | | 2015-05-26 15:06:39.762245 | FG | SIP Request | |
| 6 | Transmission Control Protocol | . Src Port: 43108 (43108 | 3), Dat Port: sips (5) | 061), Seg: 1, Ack: 1, Len: | 1001 | 2015-05-26 15:06:39.764224 | BYE | SIP Request | |
| 3 | Secure Sockets Layer | | | | | | < + | < | |
| | TLSV1 Record Layer: Applica | ation Data Protocol: sip | | | | | | | |
| | Content Type: Application | 1 Data (23) | | | | | Control | - C | |
| | Version: TLS 1.0 (0x0301) | | | | | | 24A6 92 | Store | |
| | Length: 996 | | | | | | | | |
| | Encrypted Application Dat | ta: 700ad005bfeed0ce8a6bc | :+06b7+0+d4b81acfa38bl | b863d87 | l | | | | |
| | | | | | | | | | |

3. Beside the filters, when you're capturing TLS, you need to make sure you capture the SSL handshake between the phone terminal and the VoipNow server. Otherwise, you won't be able to decrypt the capture.

Decode TLS

- 1. First you need the private key used by Kamailio. On VoipNow 3.5, you can find it in /etc/voipnow/certs/kamailio.pem.
- 2. Take the private key and save it on your PC in a filename.key file. It should look like this:

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkahkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDLsm335w5i+BiY
gg05NsBTR1ZTSbsMjkoprJoQ8KPxFvLGegwyWY+Fk25GmFCur7GfZYuYACXcU0H/
...
17DtP+PYdC2Yz61ld8F06LB6RgsZHnXlDj8yxhzeALDBRvZSt+of4iedEK1J+0pA
zuqB/sOrM+elJ8z3vsF9kikZ
-----END PRIVATE KEY----
```

Open Wireshark and go to Edit >> Preferences >> Protocols >> SSL >>Edit and do the exact setup you can see below. Use the file created earlier with the private key.

| Wireshark: Preferences - Profile: Default | | |
|---|--|--------|
| SIP | | |
| SKINNY | RSA keys list: <u>E</u> dit | |
| SMB | SSL debug file: C:\debug.txt | Browse |
| SMB2 | | |
| SML | Reassemble SSL records spanning multiple TCP segments: | |
| SMPP | Received Market States Data and States and S | |
| SMTP | Reassemble SSL Application Data spanning multiple SSL records: | |
| SNA | Message Authentication Code (MAC), ignore "mac failed": | |
| SNMP | Dra-Shared-Ker | |
| SoulSeek | Pre-shared-key. | |
| SoupBinTCP | (Pre)-Master-Secret log filename: | Browse |
| SPRT | SSI Decrypt - Profile: Default | |
| SRVLOC | | |
| SSCOP | IP address Port Protocol Key File Password | |
| SSH | 10.150.20.27 5061 sip C:\srv27.key | |
| SSL | Down | |
| STANAG 5066 | | |
| StarTeam | New | |
| STP | Edit | |
| SUA | Copy | |
| SYNCHROPHASOR | Delete | |
| T.38 | <u>Restance</u> | |
| TACACS+ | Refresh | |
| TALI | Clear | |
| TCAP | | |
| TCP | | |
| TCPENCAP + | QK Apply Cancel | |
| Help | OK Apply | Cancel |

Now, Wireshark cannot decode the capture without the SSL handshake between the phone and the server included in the capture. The handshake looks like this:

| 18 2015-05-26 15:19:39.361631 | 192.168.1.225 | TL5V1 | 10.150.20.27 | 166 Client Hello |
|-------------------------------|---------------|-------|---------------|---|
| 19 2015-05-26 15:19:39.361682 | 10.150.20.27 | TCP | 192.168.1.225 | 68 sips > 60439 [ACK] Seq=1 Ack=99 Win=14592 Len=0 TSval=3039239727 TSecr=4294944119 |
| 20 2015-05-26 15:19:39.363038 | 10.150.20.27 | TLSV1 | 192.168.1.225 | 1056 Server Hello, Certificate, Server Hello Done |
| 21 2015-05-26 15:19:39.364198 | 192.168.1.225 | TCP | 10.150.20.27 | 68 60439 > sips [ACK] seq=99 Ack=989 win=7816 Len=0 T5val=4294944119 Tsecr=3039239729 |
| 22 2015-05-26 15:19:39.773451 | 192.168.1.225 | TLSV1 | 10.150.20.27 | 382 Client Key Exchange, Change Cipher Spec, Finished |
| 23 2015-05-26 15:19:39.776366 | 10.150.20.27 | TL5V1 | 192.168.1.225 | 115 Change Cipher Spec, Finished |

This SSL handshake occurs during each phone reboot and following each TCP handshake.

At this point, the entire call flow should be visible.



Related articles

- How to create a configuration template for a certain SIP device
- · How to set up a SIP channel to interconnect with Skype forBusiness account
- Understanding SIP devices provisioning permissions
- How to set up Snom 300/320/360 SIP phones to connect to VoipNow
- How to set up Cisco/Linksys SPA phones to connect to VoipNow