Common Flaws in Encrypted VoIP

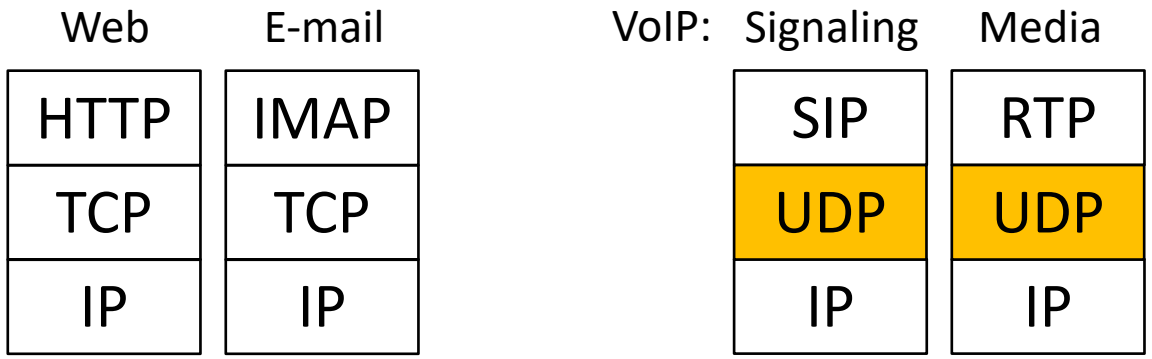
SIP-over-TLS and SDES-sRTP

March 2019

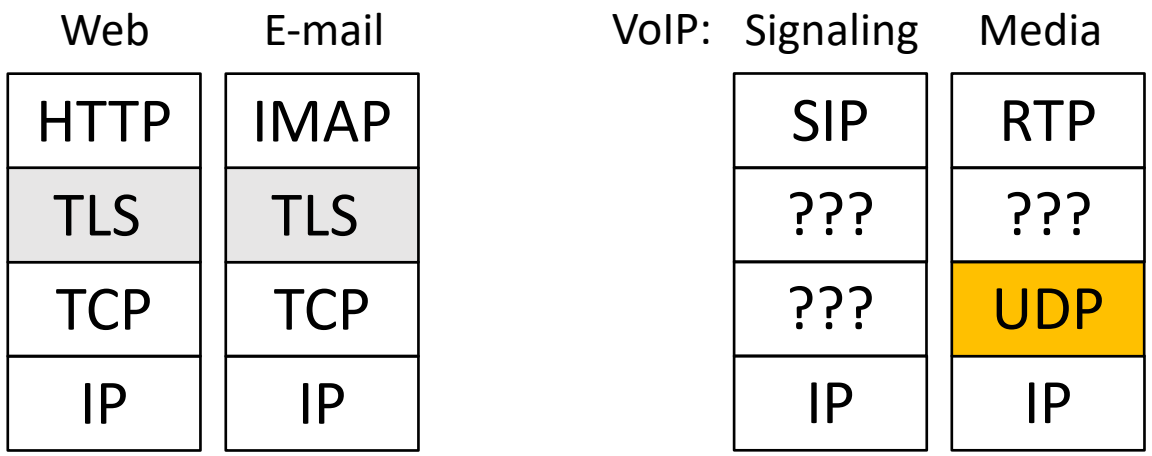
TROOPERS Next Generation Internet (NGI)

Alexander Traud

Background info: Unencrypted



Background info: Protocol Stack Add-ons



Encrypted VoIP – History of Alternatives

a) Virtual-Private Network (VPN)

   End-to-Access-Edge aka First-Hop Encryption and Authentication

b) SDES-sRTP with SIP-over-TLS

   same as VPN

c) DTLS-sRTP

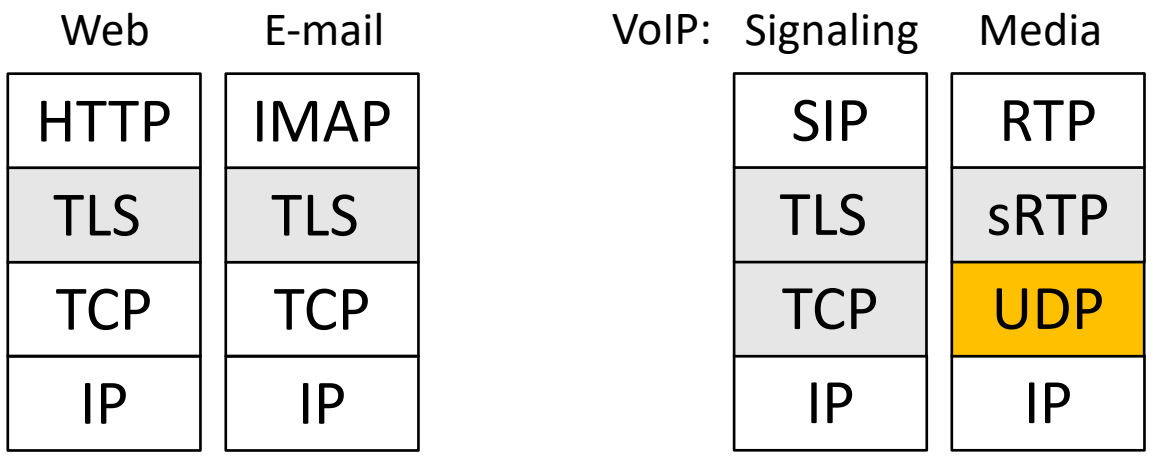
   End-to-End Encryption

d) ZRTP-sRTP

   End-to-End Encryption and Authentication: youtu.be/AmYGxwcTyQE

e) others (Skype, WhatsApp, Signal, Google Voice, …)

Background info: Protocol Stack Add-ons



VoIP Client for Mobile Phone

- **Acrobits Groundwire**
- **Belledonne Linphone**
- BroTecs Skylar
- CounterPath Bria Mobile
- Media5-fone Pro
- Mocana KeyTone Pro
- PortSIP Softphone
- Securax Zoiper
- Softil BEEHD
- Voipswitch Join
- Xnet ALL IP Home

Android:

- **VoIP By Antisip**

Nokia Mobile Phones:

i. Nokia 700: Symbian/S60
ii. Nokia 208: Series 40
iii. Nokia 503: Asha Software Platform
iv. N900 (Maemo), N9 (MeeGo): sRTP?

Linux: Jami, Jitsi, Twinkle

Bold: SDES-sRTP and DTLS-sRTP

Internet-Access Device (iAD)

- Digitalisierungsbox Basic (ZyXEL Sphairon, Bautzen)
- Digitalisierungsbox Smart (Teldat bintec-elmeg, Nürnberg)
- LANCOM 831A (Aachen)

not tested:

- DrayTek: only ZRTP?

Bold: SDES-sRTP and DTLS-sRTP

Settings available at
www.traud.de/voip

VoIP Desk-Phone

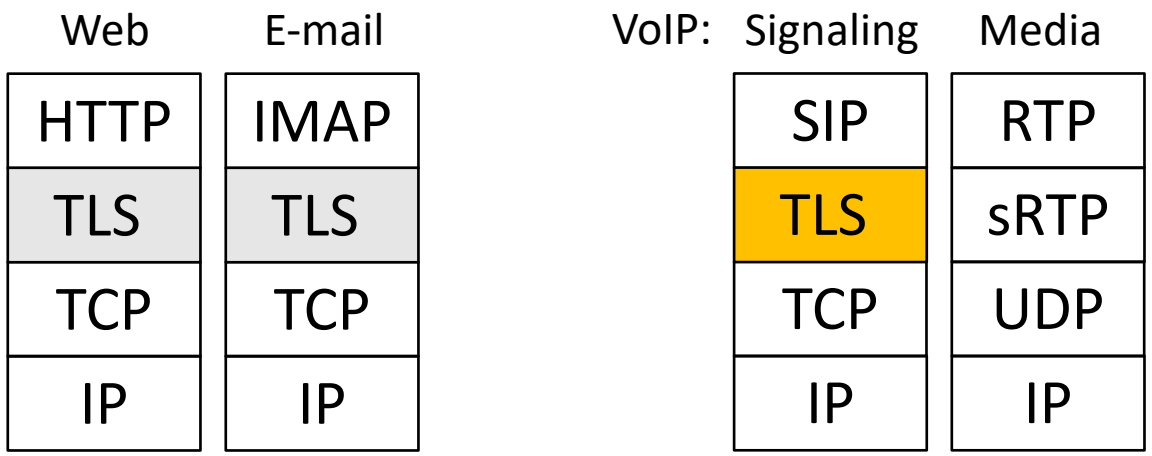
Configuration via Web interface; ‘open’ SIP possible with Digium Asterisk 13 LTS (chan_sip)

- ALE 8008 Cloud Edition DeskPhone
- Akuvox R50
- Atcom A11W
- AudioCodes 405HD
- Avaya J179
- Cisco IP Phone 7821 (SKU contains 3PCC)
- Digium D65
- Escene Univois U3S
- Fanvil X1P
- Gigaset Maxwell Basic
- Grandstream DP750
- Htek UC902
- Huawei eSpace 7950
- **innovaphone IP222**
- Mitel 6865i (former Aastra)
- Obihai OBi1022
- Panasonic KX-TGP600
- Polycom VVX 301
- RTX 9430, actually: Snom M300
- Samsung SMT-i6010
- Snom D725
- **Unify OpenScape CP200**
- VTech VSP600, actually: Snom M200 SC
- Yealink T41S

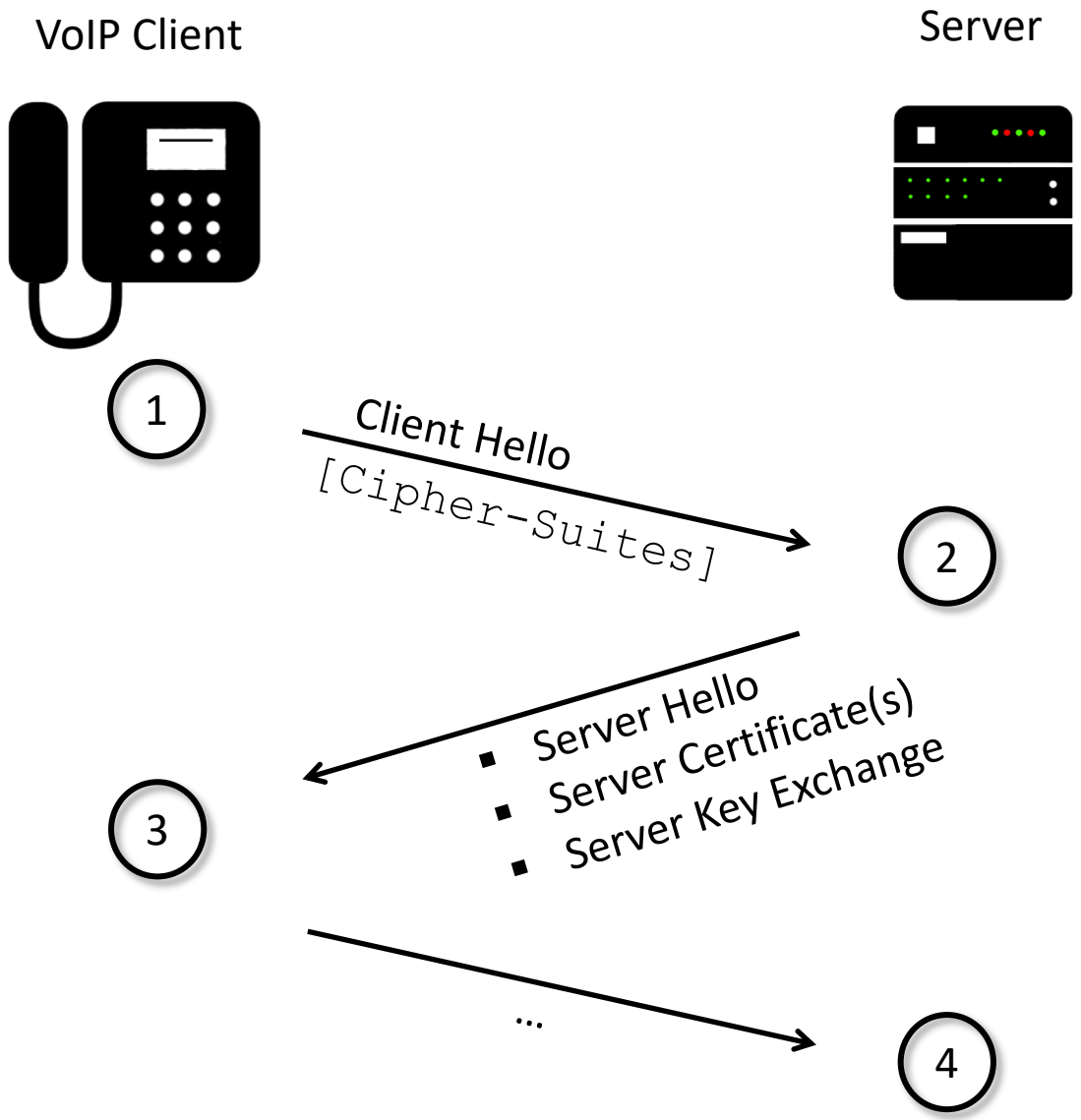
Bold: SDES-sRTP and DTLS-sRTP

Underline: 3 provided by manufacturer

Background info: Protocol Stack Add-ons



TLS Handshake: Offer, Answer



TLS Handshake: Cipher-Suites

state of the art (according Google Security Team):

01 × TLS_ECDHE_[RSA|ECDSA]_WITH_CHACHA20_POLY1305_SHA256

19 × TLS_ECDHE_[RSA|ECDSA]_WITH_AES_128_GCM_SHA256

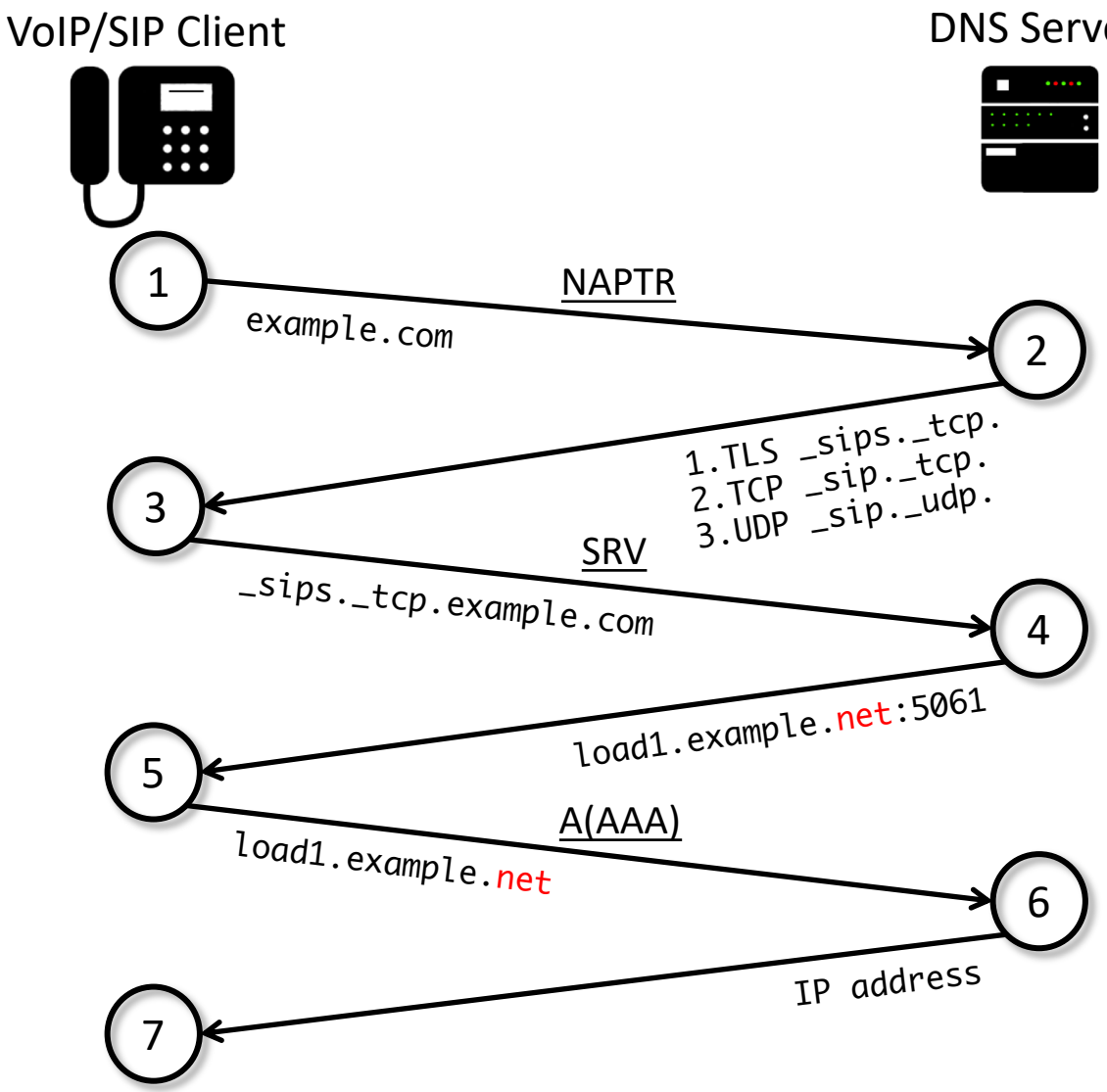
mandatory (SIP/2.0, since 2002):

–2 × TLS_RSA_WITH_AES_128_CBC_SHA

found, enabled out-of-the-box:

- Triple-DES
- RC4-SHA
- RC4-MD5
- Camellia, SEED, IDEA
- Single-DES (56 bit)
- 18 × Export (40 bit, like RC2)
- 09 × Anonymous (EC)DH = disables certificate checks
- 02 × NULL

TLS Hostname Validation: Hello, MitM!



three mistake ‘attacks’:

entered in phone

- local IP instead of hostname
- wrong hostname (A) like
  `proxy.dus.net`
- wrong hostname (SRV)

> 20 phones connected

more attacks in:

doi.org/10.1145/2382196.2382204

TLS Trust-Anchors buried in

- with outdated CAs
  Symantec, StartCom, legacy 1024 bit, private test certificates, …
- with outdated intermediates
  match before CA → chain of trust fails
- with invisible CAs

user/admin not allowed to disable/replace those

Configuration hurdles, while adding own CA:

2 × not PEM (Base64), not DER (binary), but PKCS12 (cert + private key)

TLS Trust-Anchors: Not with me!

Manufacturer confirmed:

- Digium: no certificate handling
- Unify (former Siemens Enterprise): DLS required (‘free’ for Windows)

Manufacturer denies visible feature in user interface:

- Samsung

Failed to configure:

- bintec-elmeg: button to enable validation; where to put trust anchor?

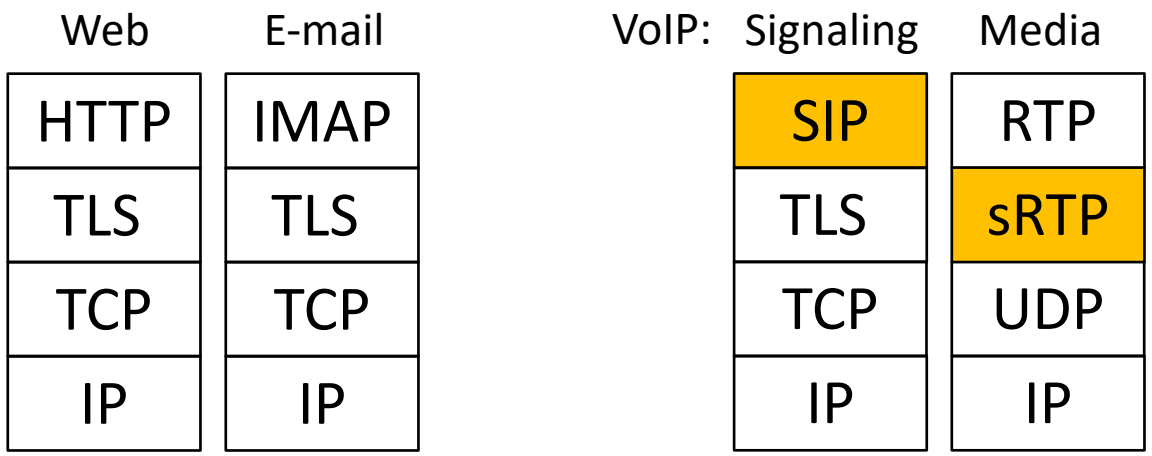
SSL/TLS Library outdated …

… or just its configuration?

01 × no TLS 1.2
>1 × no Cipher Suites based on AEAD like GCM; just CBC
>1 × no Cipher Suites with Forward Secrecy (PFS)
01 × Certificate Revocation (OCSP, CRL)

Wildest errors:
SHA-384 based certificates fail, SHA-256 work

Background info: Protocol Stack Add-ons



SDES-sRTP Weak Key

```
a=crypto:1 AES_CM_128_HMAC_SHA1_80 \
inline:MTE1ODA3NzMxMQAAAAAAAAAAAAAAAAAAAAAA
```

should be 128bit AES key + 112bit salt, Base64:
bytes in hex: 31 31 35 38 30 37 37 33 31 31 00 00 00 …
human readable: 1158077311\00\00\00 …

Mistakes of others:

a) everything is a digit
b) everything is hex (character range: 0-9 and a-f) = 64 bit
c) every x^{th} byte is \00 (x = 2, …) = -8 bit for each NULL
d) every 8^{th} bit is zero always (character range: US-ASCII) = 112 bit

Audio-Codec: Variable Bitrate (VBR)

RFC 7587 section 3.1.2

extract speech because of size of RTP packets

Mitigation:

a) disable Speex and Opus Codec
b) go for Constant Bitrate (CBR)
c) padding bits

→ Padlock icon in display of remote phone

Interoperability: Call Drops thanks to sRTP

Example for Ubuntu 18.04 LTS:
www.ippf.eu/threads/251629

tested with Digium Asterisk 13 LTS, channel driver `chan_sip`

- `tlsenable=yes`
- `nat=force_rport,comedia` ;one approach for phones behind NAT
- `directmedia=no` ;Media-Plane Back-to-Back User Agent (B2BUA)

SIP Session Timers (RFC 4028, since 2005), enabled on default (`=accept`)

- `session-timers=originate`
- `compactheaders=yes` ; just for fun to reduce (mobile) data

→ in some phones, re-INVITE resets RTP-SEQ

→ in some phones, re-INVITE resets sRTP-ROC

→ some phones cannot parse/ignore compact session headers

Interoperability: Call Drops thanks to sRTP

Lesson learned, until phones are fixed:

- `session-timers=refuse`

VoIP/SIP Providers with SIP-over-TLS and SDES-sRTP:

1. dus.net
   Media-Plane B2BUA = always between
2. Easybell
   SIP Proxy = other party must have it → select in phone: sRTP best-effort|optional
3. Telekom Deutschland
   a) SIP Proxy = other party must have it → select in phone: sRTP best-effort|optional
   b) Session-Border Controller (SBC): MediaSec Extension
4. Google Voice

sRTP Padlock Icon like Web browsers

a) if sRTP

SDES-sRTP requires an encrypted signaling channel: SIP-over-TLS
– optional sRTP: active attacker upgrades connection, injects icon
– DNS-NAPTR: active attacker downgrades connection, keeps icon

b) if SDES-sRTP and SIP-over-TLS

encrypted and authenticated: Certificate/Hostname Validation

c) Signaling: insecure, weak, strong Cipher Suite, Public Key, Hash, …

d) Media: Opus with VBR, weak AES key

→ What about an Open Padlock Icon with INFO button?

→ no icon, when everything looks good

→→ reveals misconfigurations and insecure implementations!

Experiences with Responsible Disclosure

Want to report a Security Vulnerability.

You're not coming in!

Want to report a Security Vulnerability.

For which company do you work for?

Private Individual

How many phones do you have?

One

Change switch a on tab g to the value u – we do not document that!

Lessons learned

- Manufacturer
  - security is not a one-time project
  - instead a continuous topic

  “When we added (D)TLS 1.2, there was no requirement to add AEAD ciphers.”
- Purchasers
  - Data Sheet: sRTP … SIP-over-TLS
  - What does it really mean? Why not look at the user interface / status icons?
- Administrators
  - heroes, super(wo)men
  - shall they test all this?
  - when you are back in your company, give them a hug!