

# PENETRATION TESTING A VOIP ENVIRONMENT WITH WIREBUG



# AGENDA



- Where is VoIP used?
- Basic VoIP technology
- VoIP nowadays
- How to pentest VoIP?
- WireBug toolset
- Getting network access
- Getting a man-in-the-middle Position
- Eavesdropping a call
- Encryption methods
- Decrypt and downgrade encrypted calls
- Conclusion & recommendation
- Q & A

# WHERE IS VOIP USED?



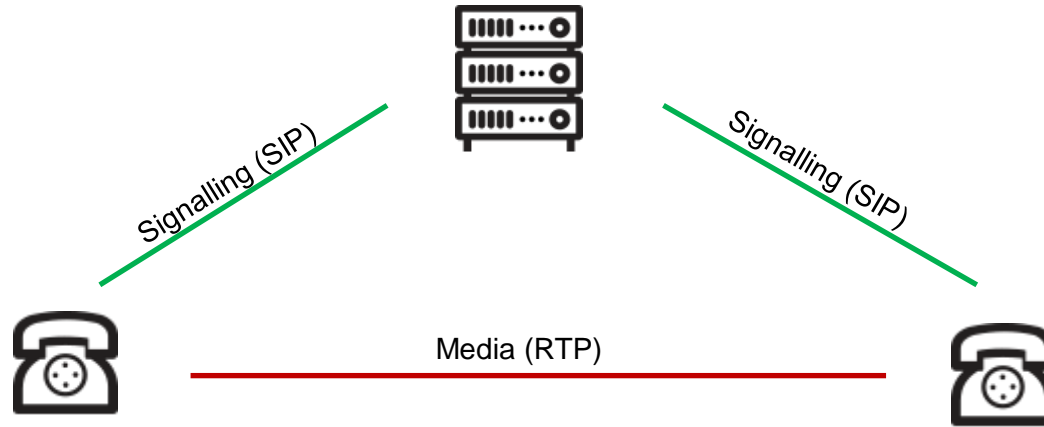
(Source: <https://amayei.nyc3.digitaloceanspaces.com/2018/09/Donald-Trump-Telephone.jpg>)

# WHERE IS VOIP USED?



- Majority of companies (EU)
- ~ 35 million public VoIP trunks throughout Germany
- 2020 end of life for old trunks (statement German ITSP providers)
- IoT & Industry 4.0
- In times of the coronavirus > home office & online conferences

# BASIC VOIP TECHNOLOGY



# VOIP NOWADAYS



Cooperations



Federation

Provider



SIP Trunk

Branch



VoIP-Phone  
Branch



PBX-Branch

Anywhere  
Workplace



VoIP-Phone  
FAE

Headquarter



Database



Media gateway



PBX-Standby



PBX-Master



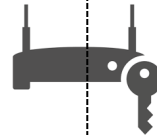
Active Directory



Skype for  
Business



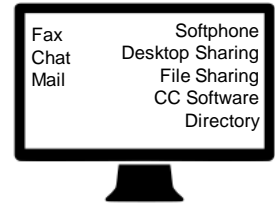
Application server:  
Fax  
Reporting  
Voicemail  
Contact Center  
Backups  
...



Session Border Controller



VoIP-Phone



# VOIP NOWADAYS



Cooperations



Federation

Provider



SIP Trunk

Branch



VoIP-Phone  
Branch



PBX-Branch

Anywhere  
Workplace



VoIP-Phone  
FAE

Headquarter



Active Directory



Media gateway



PBX-Standby



PBX-Master



Skype for  
Business



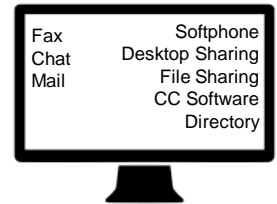
Application server:  
Fax  
Reporting  
Voicemail  
Contact Center  
Backups  
...



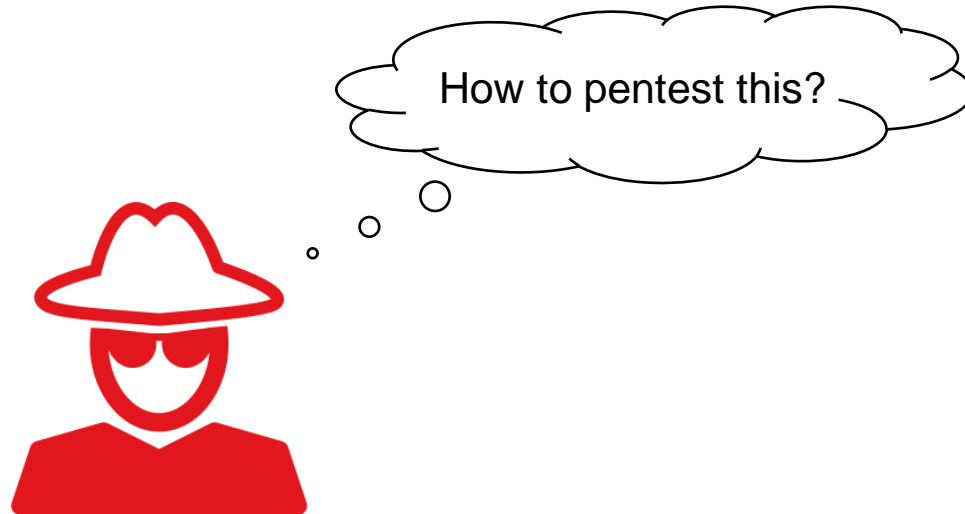
Session Border Controller



VoIP-Phone



**SECURE?!**





# CURRENT MARKET SITUATION

- Only few tools available
- Outdated or not working tools
- Low adaptability





# GETTING NETWORK ACCESS



- Network separation
- Auto VLAN assignment via LLDP-MED (802.1AB)
- Layer 2 based protocol without any authentication



# LLDP-MED (802.1AB)



```
‣ Frame 1515: 116 bytes on wire (928 bits), 116 bytes captured (928 bits)
‣ Ethernet II, Src: UnifySof_00:87:24 (00:1a:e8:00:87:24), Dst: LLDP_Multicast (01:80:c2:00:00:0e)
‣ Link Layer Discovery Protocol
  ‣ Chassis Subtype = Network address, Id: fe80::21a:e8ff:fe79:8823
  ‣ Port Subtype = MAC address, Id: 00:1a:e8:00:87:24
  ‣ Time To Live = 120 sec
  ‣ Capabilities
  ‣ Ieee 802.3 - MAC/PHY Configuration/Status
  ‣ Telecommunications Industry Association TR-41 Committee - Media Capabilities
  ‣ Telecommunications Industry Association TR-41 Committee - Network Policy
  ‣ Telecommunications Industry Association TR-41 Committee - Network Policy
  ‣ Telecommunications Industry Association TR-41 Committee - Network Policy
  ‣ Telecommunications Industry Association TR-41 Committee - Extended Power-via-MDI
  ‣ End of LLDPDU
```

Self-crafted Unify VoIP Phone LLDP packet

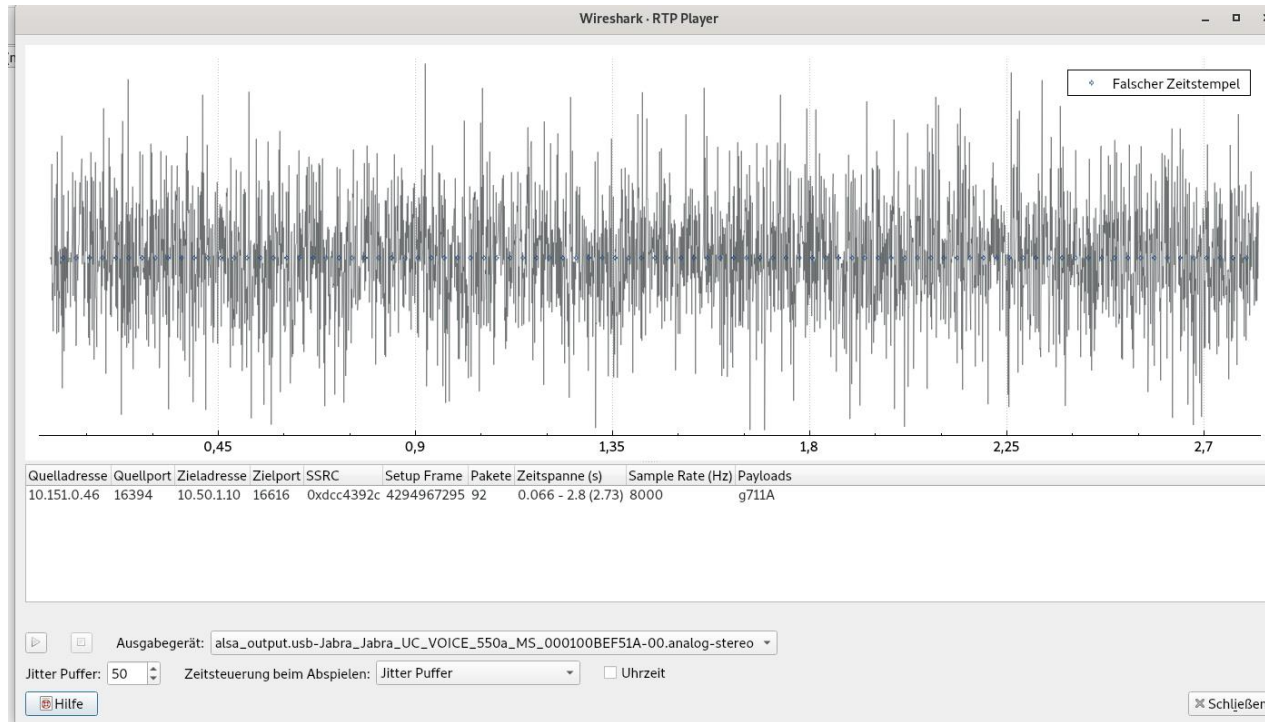


# GETTING A MITM POSITION

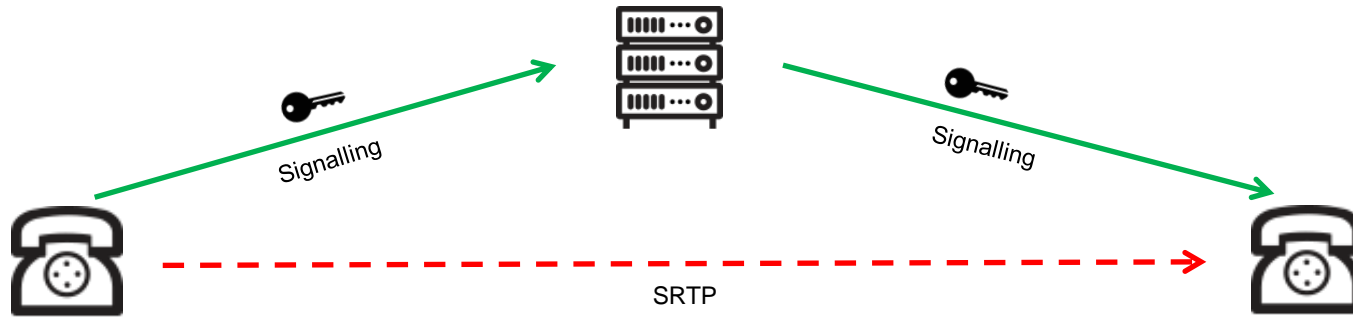


802.1Q  
802.1X  
802.1D  
802.1AB

# EAVESDROPPING A VOIP CALL

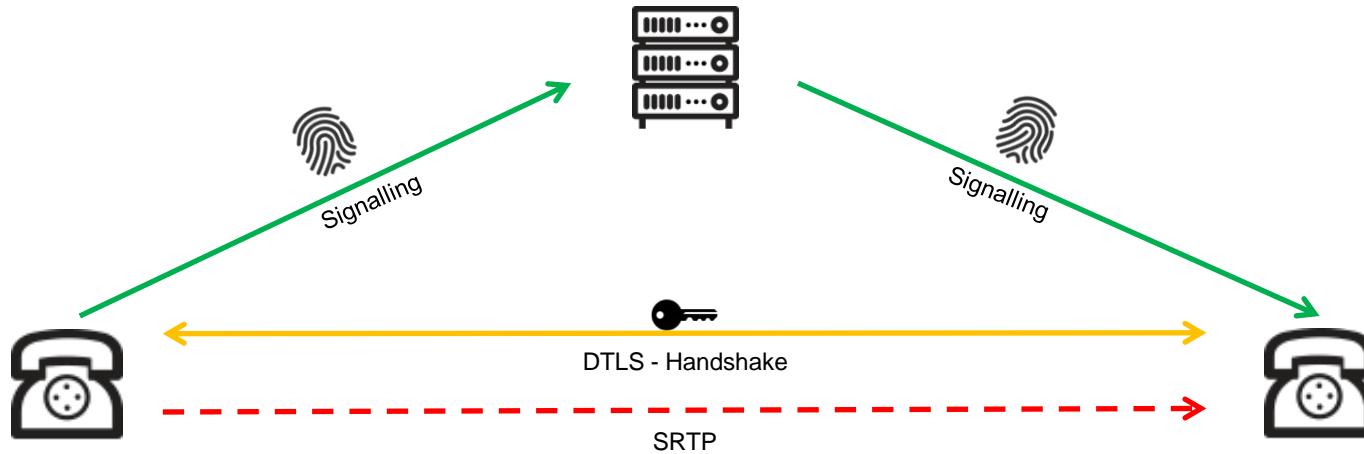


# SRTP-SDES

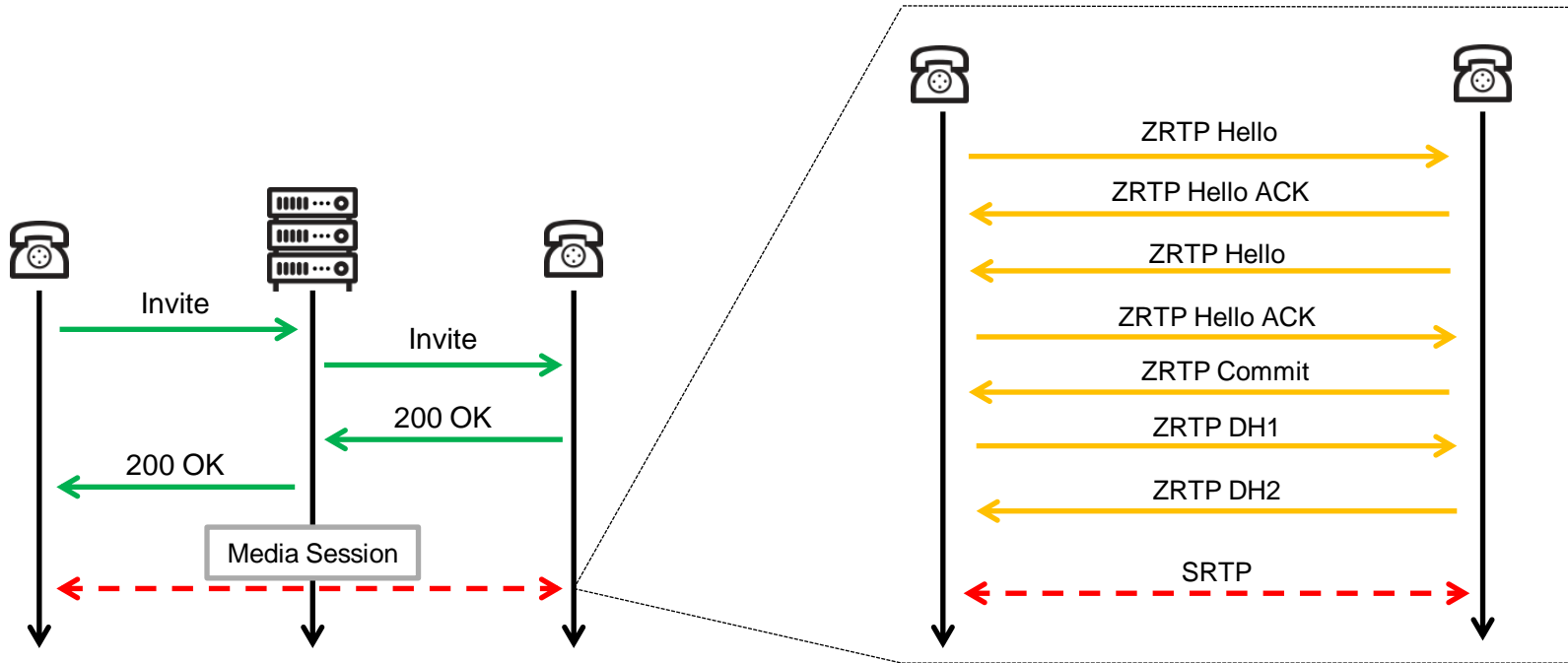




# SRTP-DTLS



# ZRTP

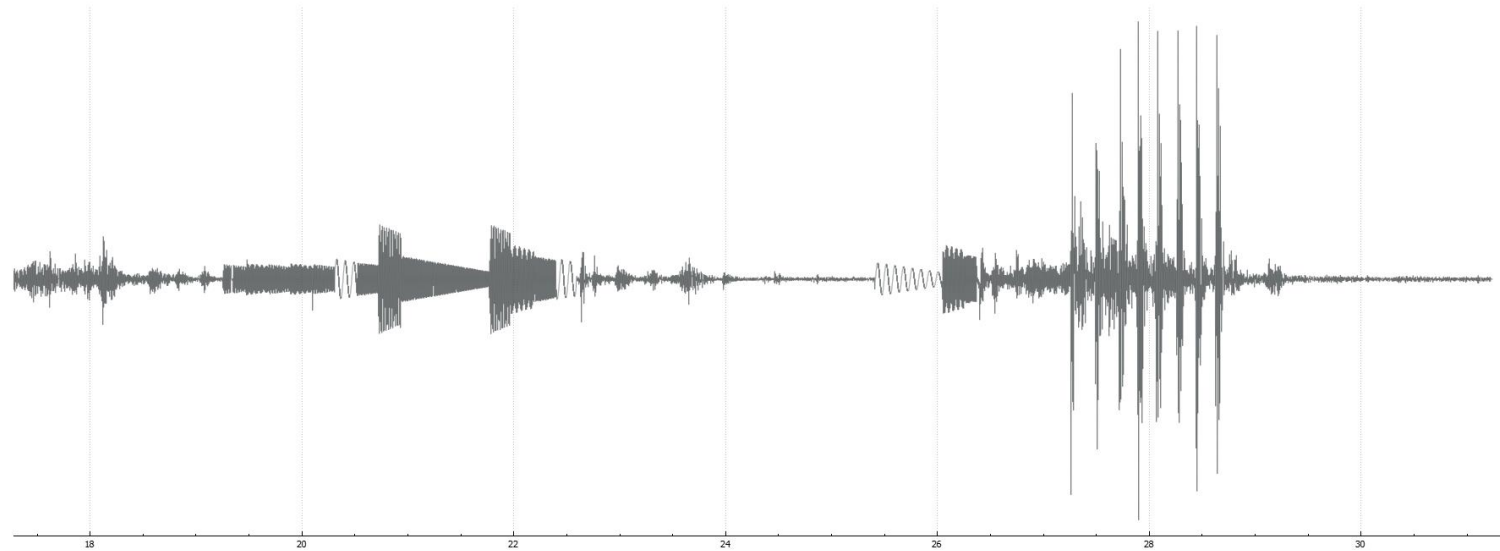


# EXTRACTING THE AES KEY FROM SIP



```
> Frame 13: 1171 bytes on wire (9368 bits), 1171 bytes captured (9368 bits) on interface 0
> Ethernet II, Src: RealtekU_00:10:11 (52:54:00:00:10:11), Dst: RealtekU_c9:70:85 (52:54:00:c9:70:85)
> Internet Protocol Version 4, Src: 192.168.122.183, Dst: 192.168.122.168
> Transmission Control Protocol, Src Port: 5060, Dst Port: 63290, Seq: 1026, Ack: 1180, Len: 1117
▼ Session Initiation Protocol (200)
  > Status-Line: SIP/2.0 200 OK
  > Message Header
  ▼ Message Body
    ▼ Session Description Protocol
      Session Description Protocol Version (v): 0
      > Owner/Creator, Session Id (o): - 1324708577 1 IN IP4 192.168.122.183
      Session Name (s): SIPPER for PhonerLite
      > Connection Information (c): IN IP4 192.168.122.183
      > Time Description, active time (t): 0 0
      > Media Description, name and address (m): audio 5062 RTP/AVP 8 0 3 9 18 101
      > Media Attribute (a): rtpmap:8 PCMA/8000
      > Media Attribute (a): rtpmap:0 PCMU/8000
      > Media Attribute (a): rtpmap:3 GSM/8000
      > Media Attribute (a): rtpmap:9 G722/8000
      > Media Attribute (a): rtpmap:18 G729/8000
      > Media Attribute (a): fmp:18 annexb=yes
      > Media Attribute (a): rtpmap:101 telephone-event/8000
      > Media Attribute (a): fmp:101 0-16
      > Media Attribute (a): crypto:1 AES_CM_128_HMAC_SHA1_80 inline:rqA21ZvC5f42wB6v60ClJH5amG0gkXC38PTPVwZ
      > Media Attribute (a): ssrc:1076816332
      Media Attribute (a): sendrecv
      [Generated Call-ID: 002BA3D1-B572-EA11-B941-A0AFCB9F7763@192.168.122.168]
```

# DECRYPTED RTP DATA



# DOWNGRADE ZRTP TO PLAIN RTP



- Intercept UDP traffic between the endpoints
- Drop the ZRTP initial packets
- Fallback to plain RTP

# CONCLUSION & RECOMMENDATION



- Conclusion:
  - SySS developed a toolset for VoIP & UC pentesting
  - There is a large area of attack
  - VoIP != VoIP
  - Tons of configuration and implementation flaws
  
- Recommendation:
  - Check the implementation and the security whitepapers of manufacturers
  - Spend time to your security concept for VoIP & UC
  - Penetration tests

# Q & A



## PENTEST

State-of-the-Art of IT System  
Intrusion



## DIGITAL FORENSICS

Addressing Threats -  
Gathering Evidence



## RED TEAMING

Simulating APT -  
Improving Resistance



## LIVE HACKING

Experiencing Attacks -  
Raising Awareness



## TRAINING

Practising Safety -  
Improving Competence

### Contact me:

Moritz Abrell  
moritz.abrell@syss.de  
+49 (0)7071 – 40 78 56-6135

### Visit us:

<https://www.syss.de>  
'[https://www.youtube.com/SySS Pentest TV](https://www.youtube.com/SySS%20Pentest%20TV)'  
<https://github.com/SySS-Research>

THE PENTEST EXPERTS

[WWW.SYSS.DE](http://WWW.SYSS.DE)