# 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

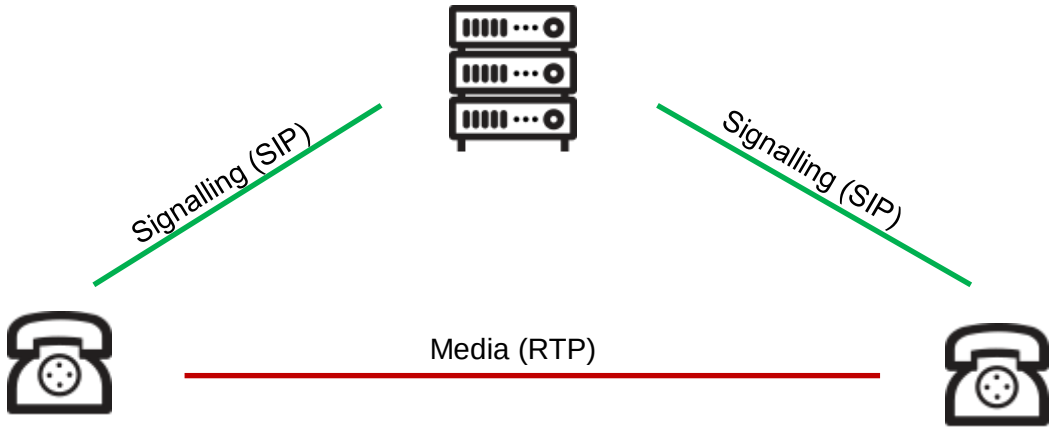
# WHERE IS VOIP USED?

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

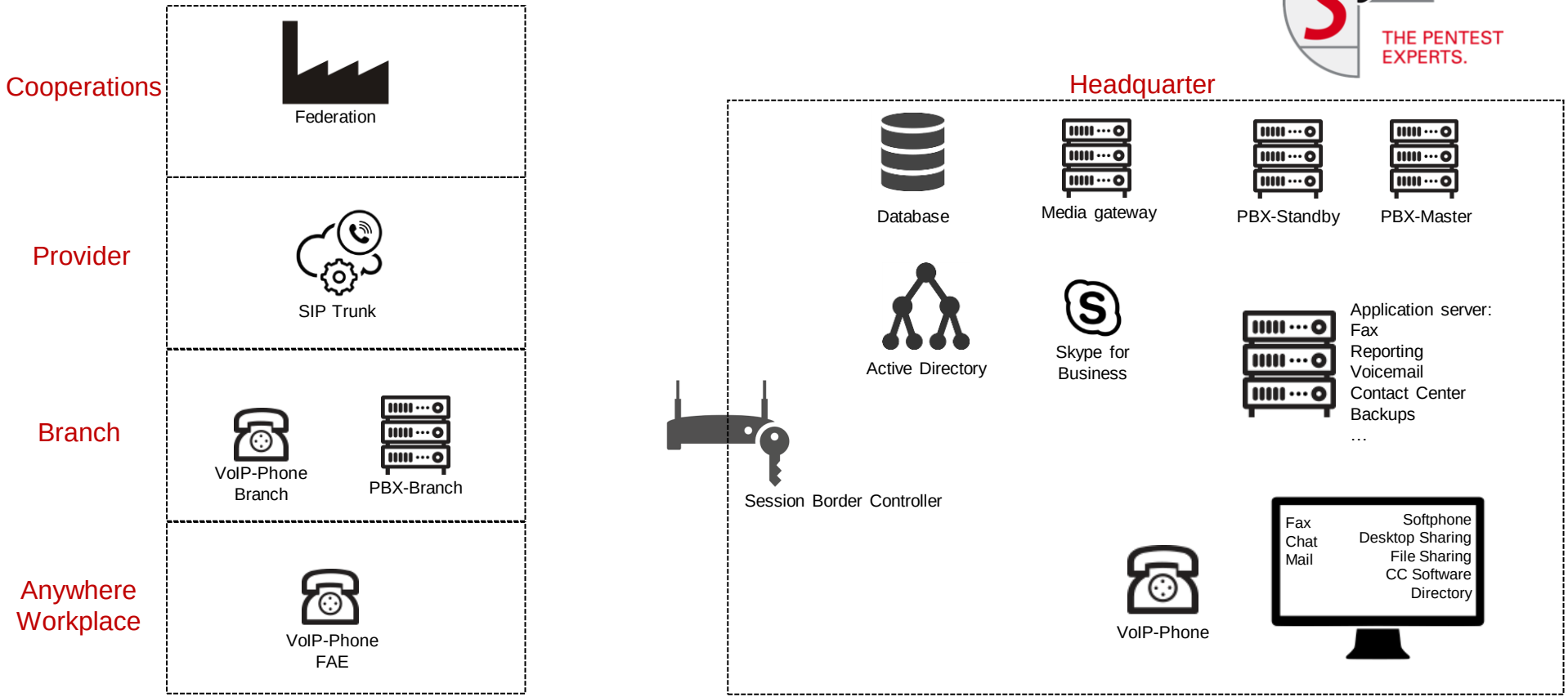
# WHERE IS VOIP USED?

- → 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

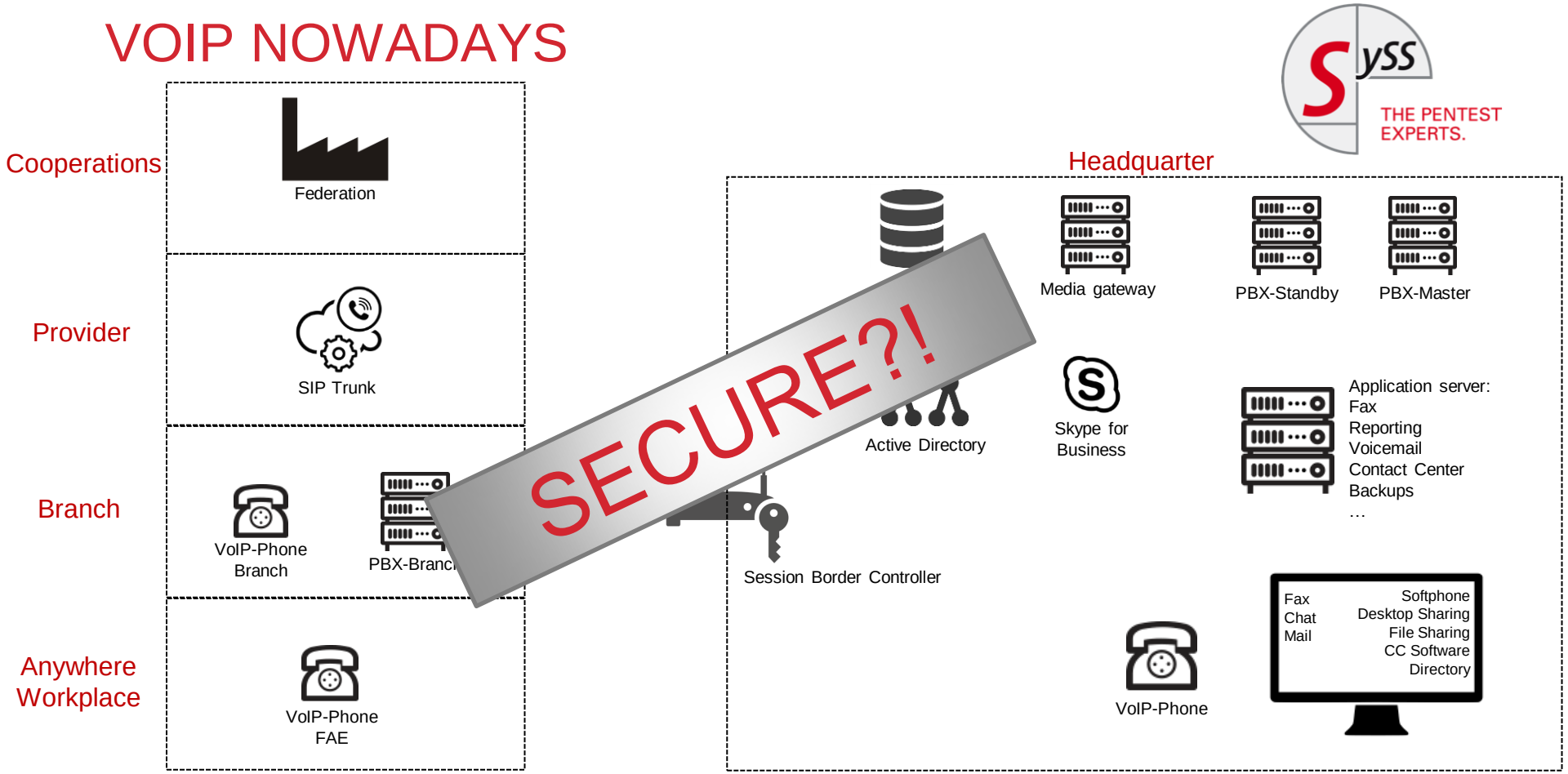
# BASIC VOIP TECHNOLOGY

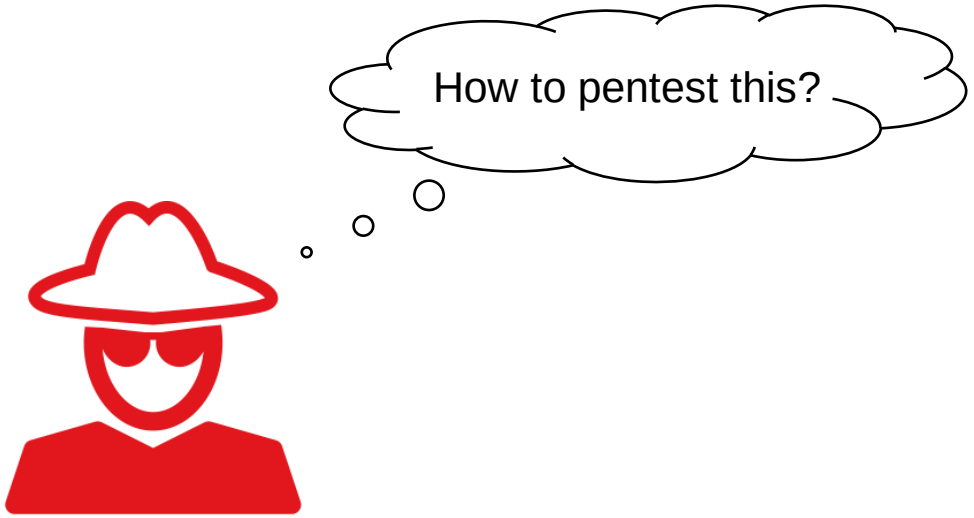


# VOIP NOWADAYS



# VOIP NOWADAYS




How to pentest this?

# CURRENT MARKET SITUATION

THE PENTEST EXPERTS.

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- → Outdated or not working tools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

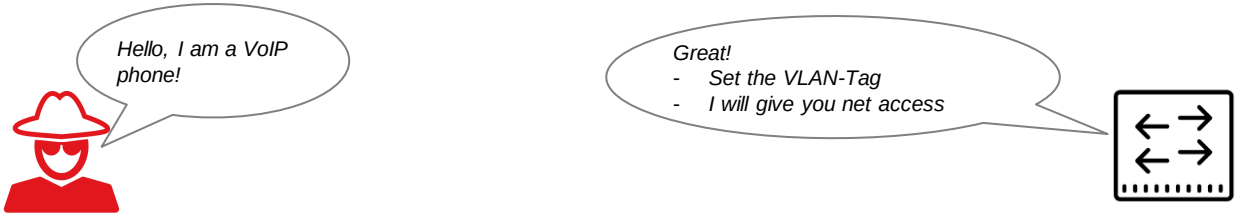
# WIREBUG – A VOIP PENTEST TOOLSET

THE PENTEST EXPERTS.

- → Toolset containing a handful python and shell s scripts for pentesting a VoIP environment
- → Wizard function for easy usage
- → Getting network access
- → Discover VoIP networks
- → Getting Man-in-the-Middle Positions
- → Lateral movement

# GETTING NETWORK ACCESS

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

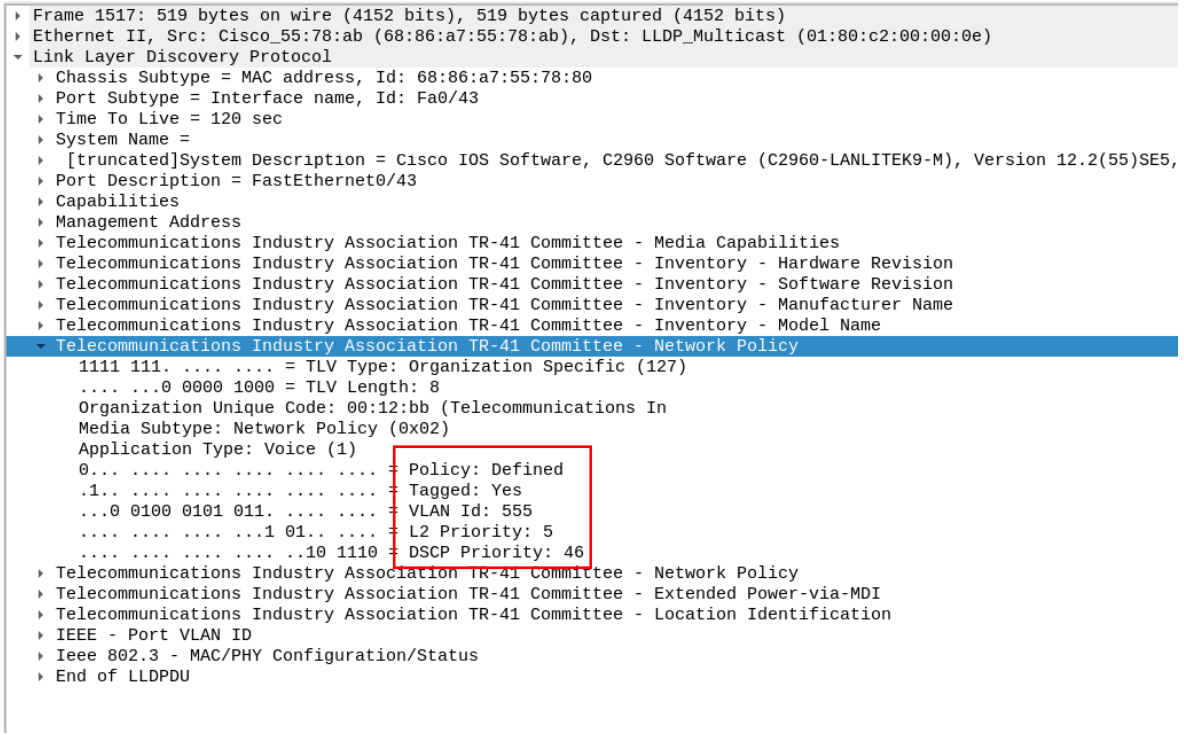


# LLDP-MED (802.1AB)

```
▸ 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

# LLDP-MED (802.1AB)

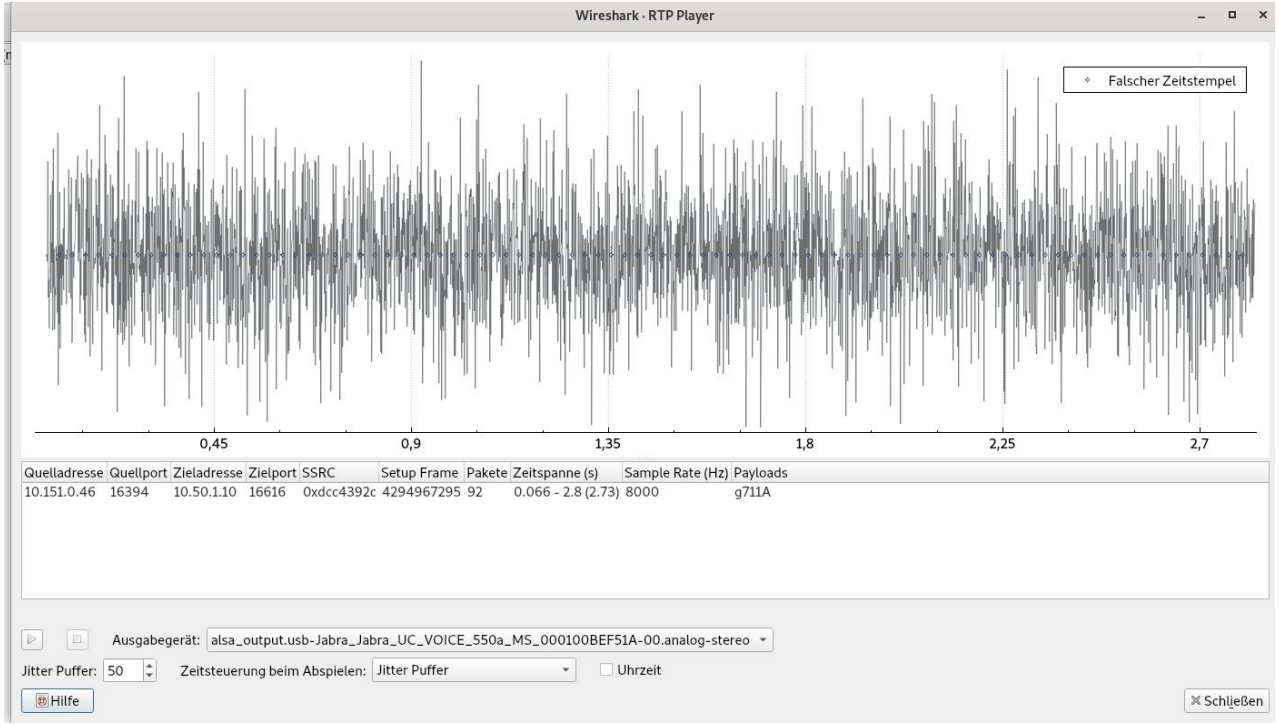



Response from the network switch

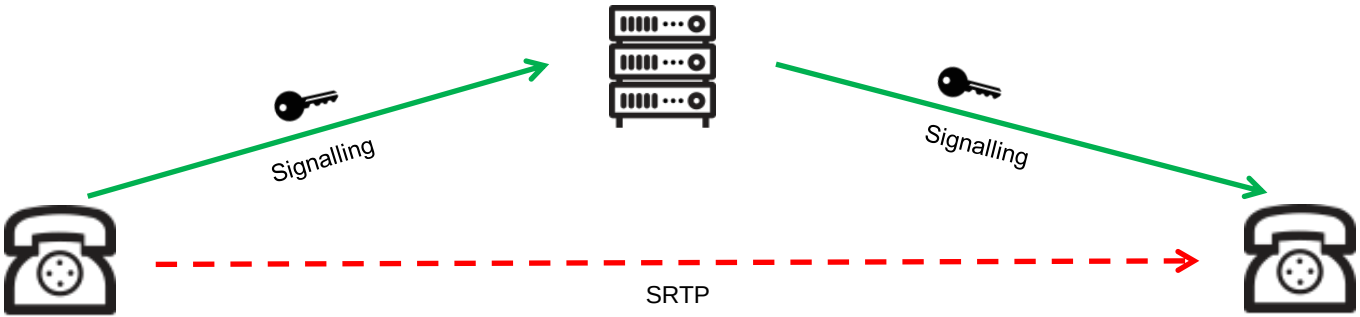
# GETTING A MITM POSITION

802.1Q
802.1X
802.1D
802.1AB

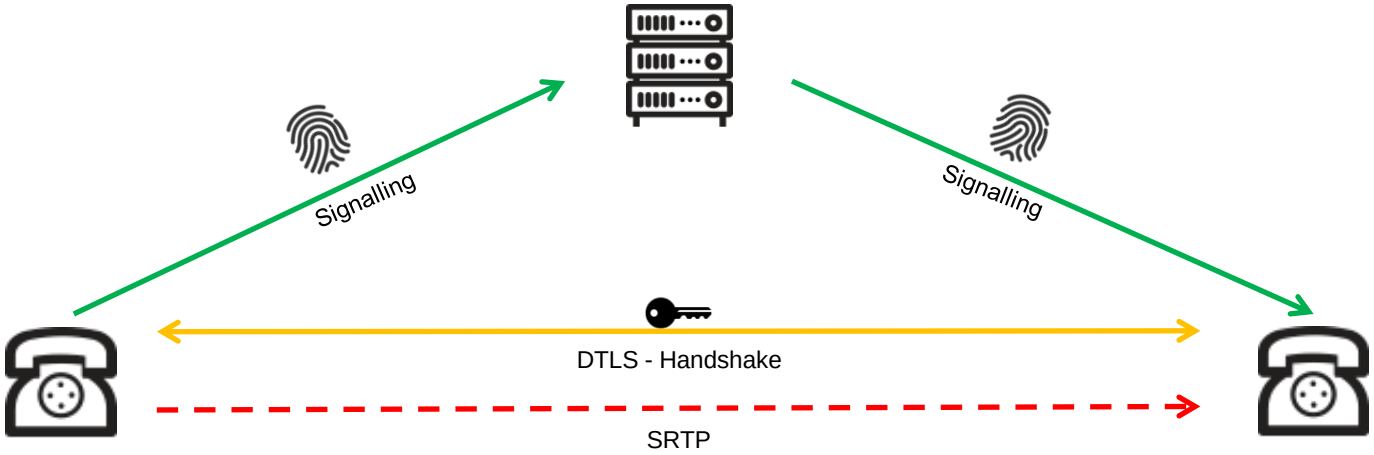
# EAVESDROPPING A VOIP CALL



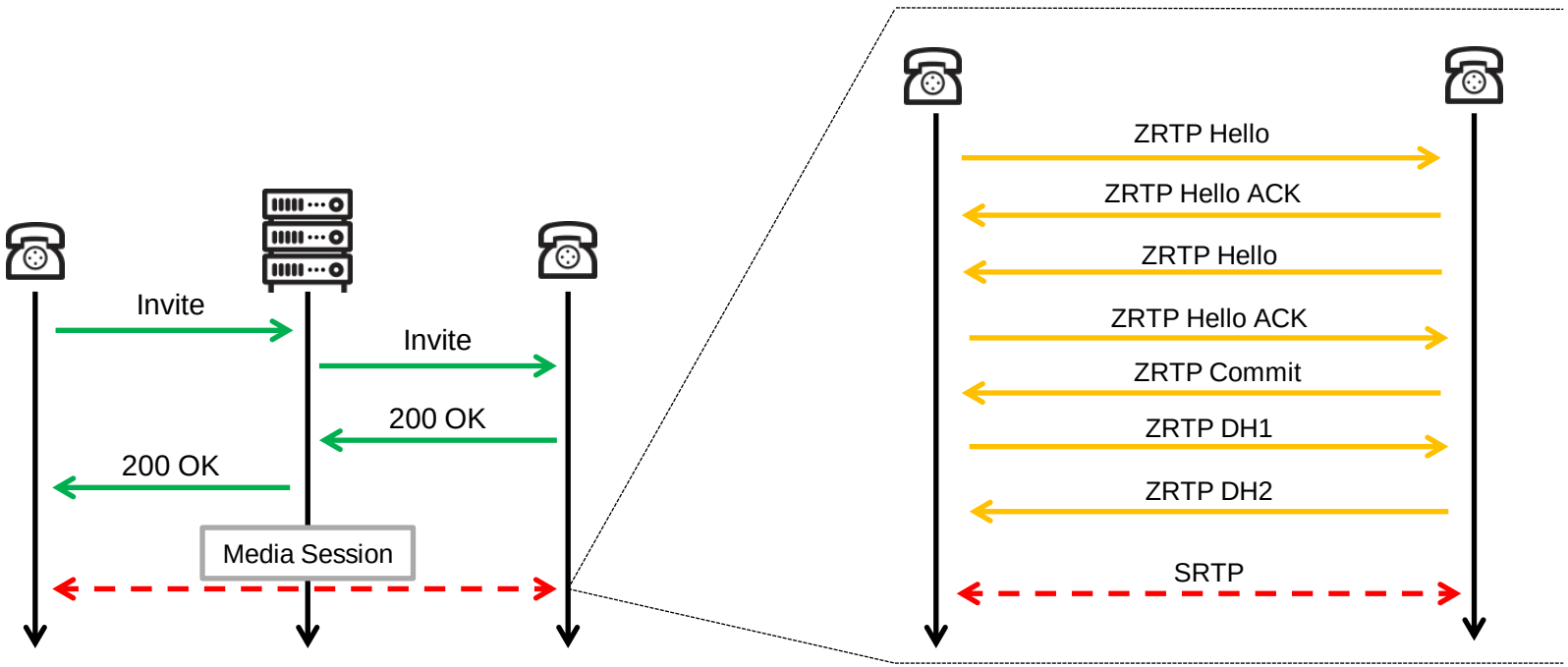
# SRTP-SDES



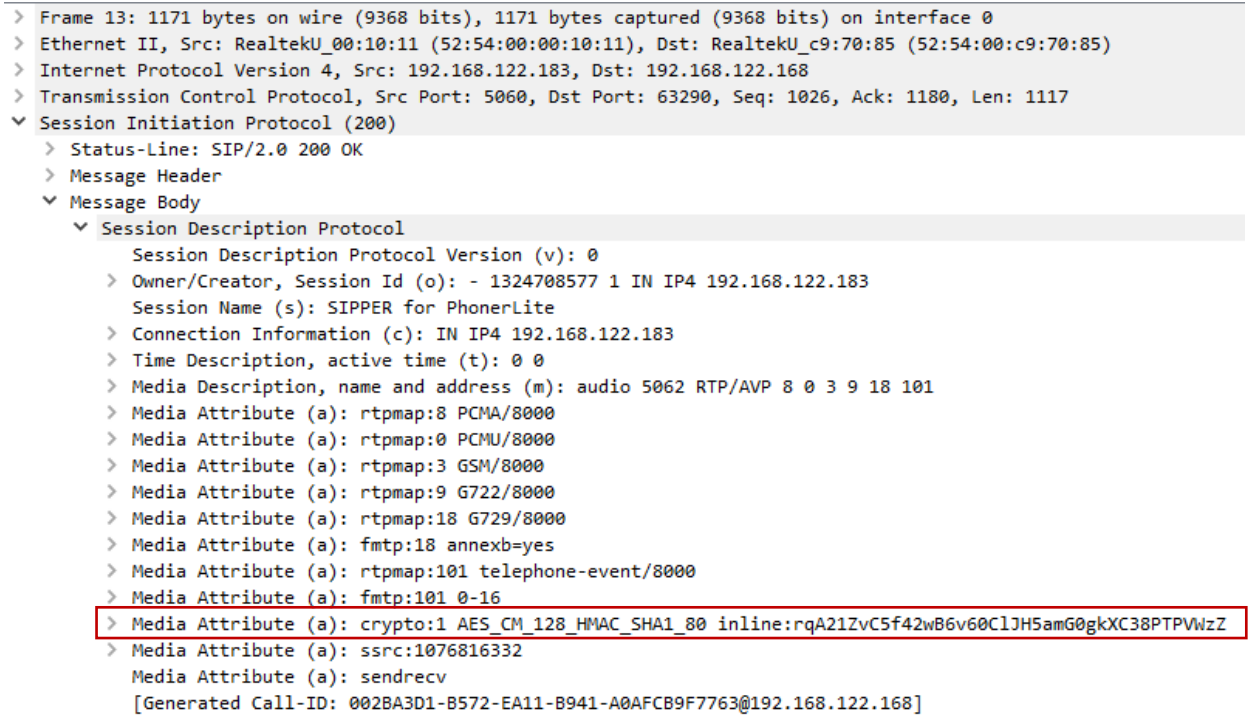
# SRTP-DTLS



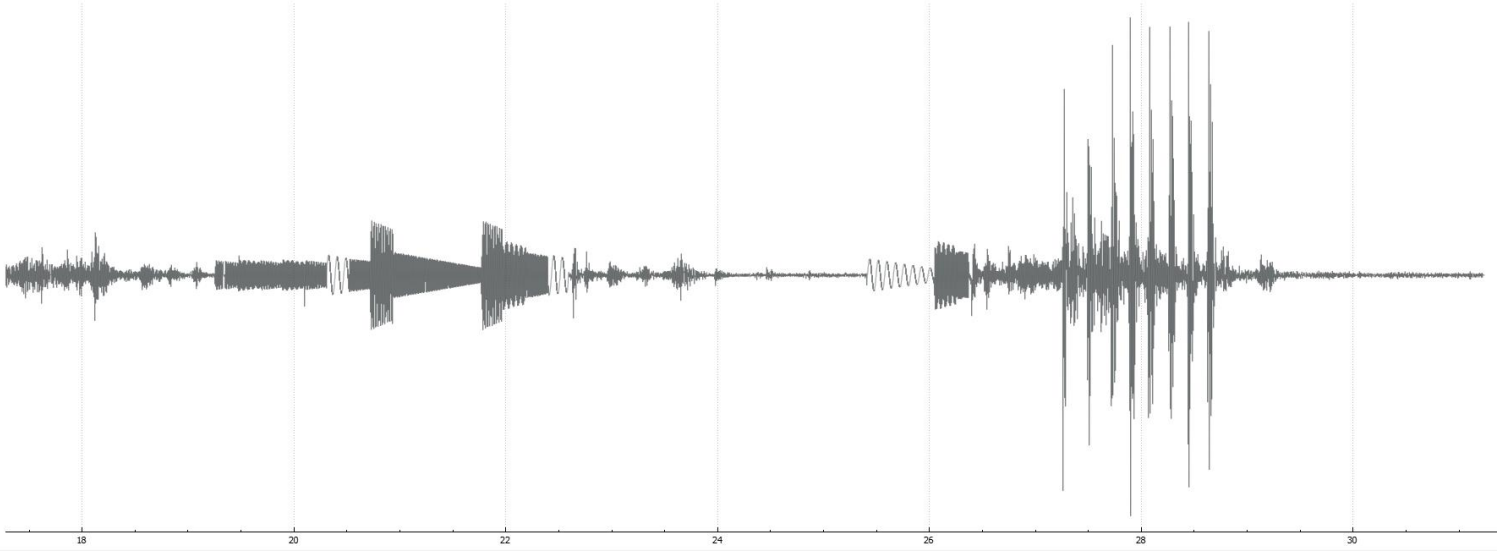
# ZRTP


Invite
Invite
200 OK
200 OK
Media Session
ZRTP Hello
ZRTP Hello ACK
ZRTP Hello
ZRTP Hello ACK
ZRTP Commit
ZRTP DH1
ZRTP DH2
SRTP

# EXTRACTING THE AES KEY FROM SIP



# 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

THE PENTEST EXPERTS.

- 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

THE PENTEST EXPERTS.

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://github.com/SySS-Research

THE PENTEST EXPERTS

WWW.SYSS.DE