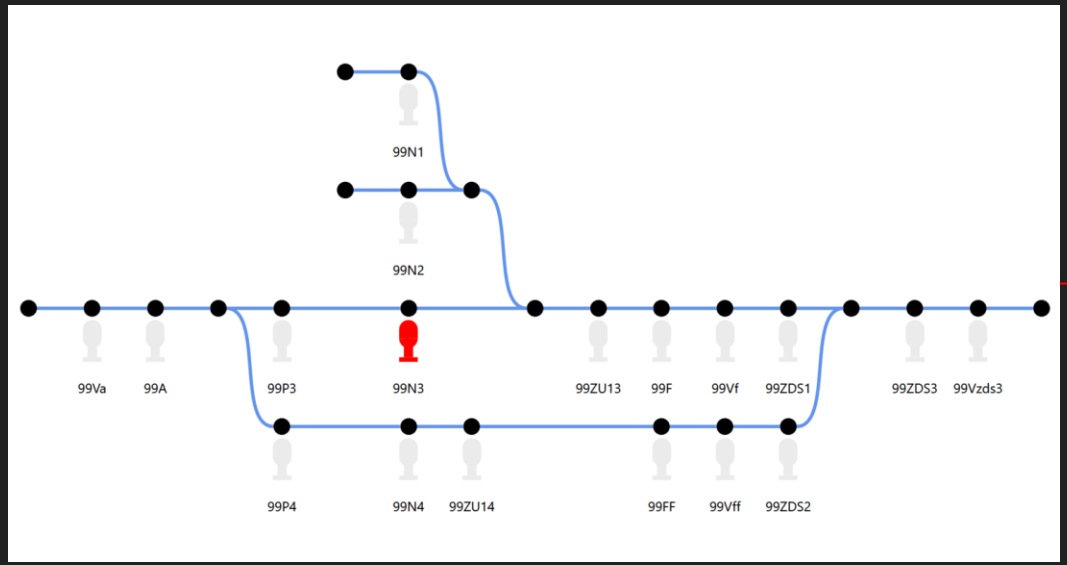
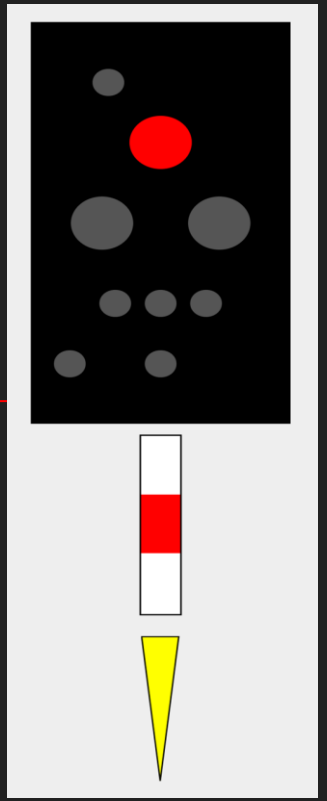
Hackathon IT-Security

Oder: Der Unterschied zwischen Safety und Security

1. RaSTA Safety Protokoll - Sicherheitsanalyse

Angreifermodell und Ziele des Angreifers

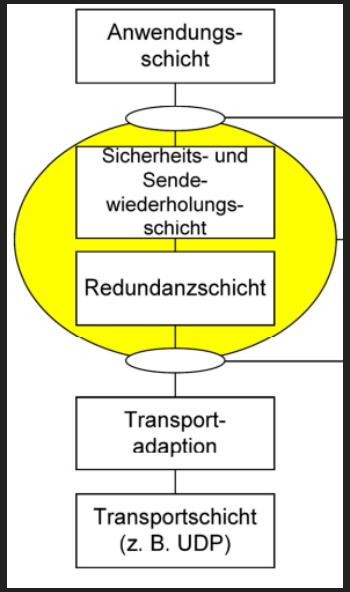


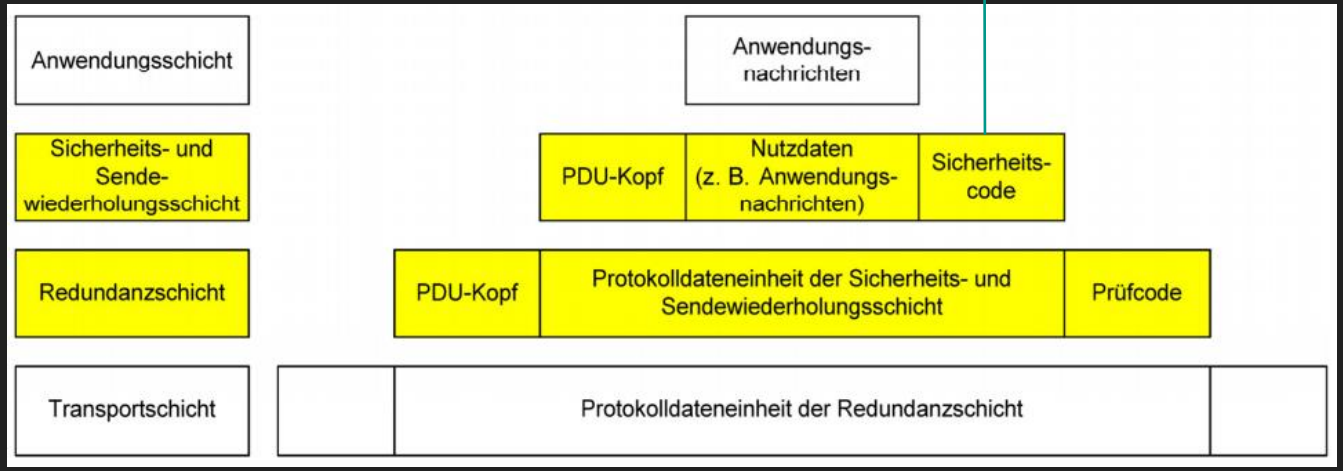


RaSTA-Angriffe - Replay-Angriff

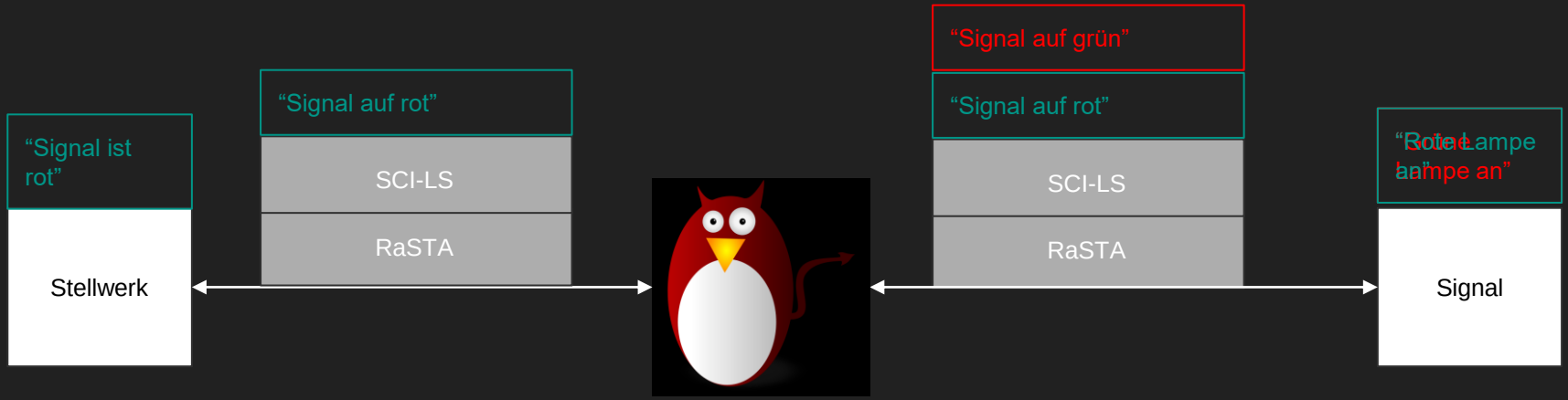
RaSTA-Angriffe - Replay-Angriff

RaSTA-Angriffe - Passwort-Wiederherstellung



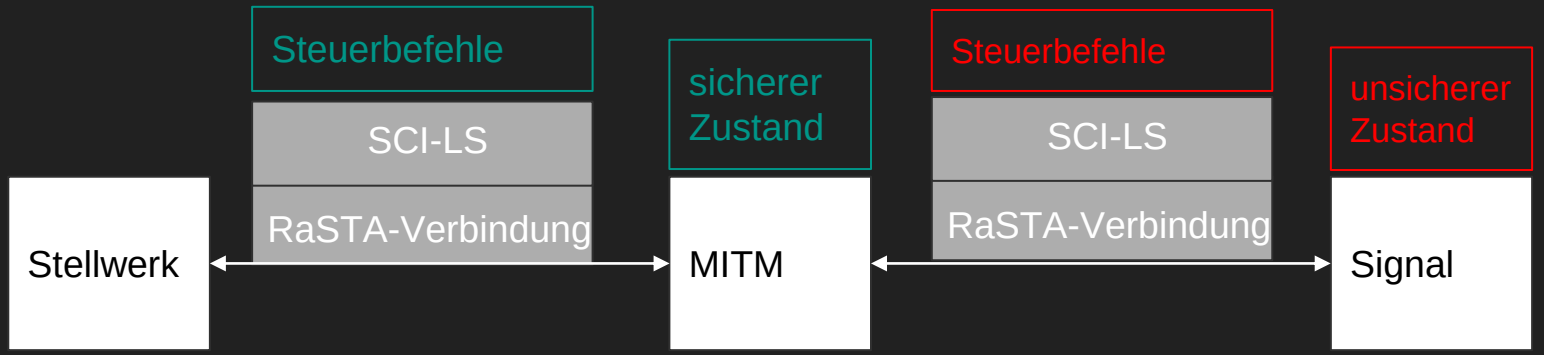


RaSTA-Angriffe - Length Extension

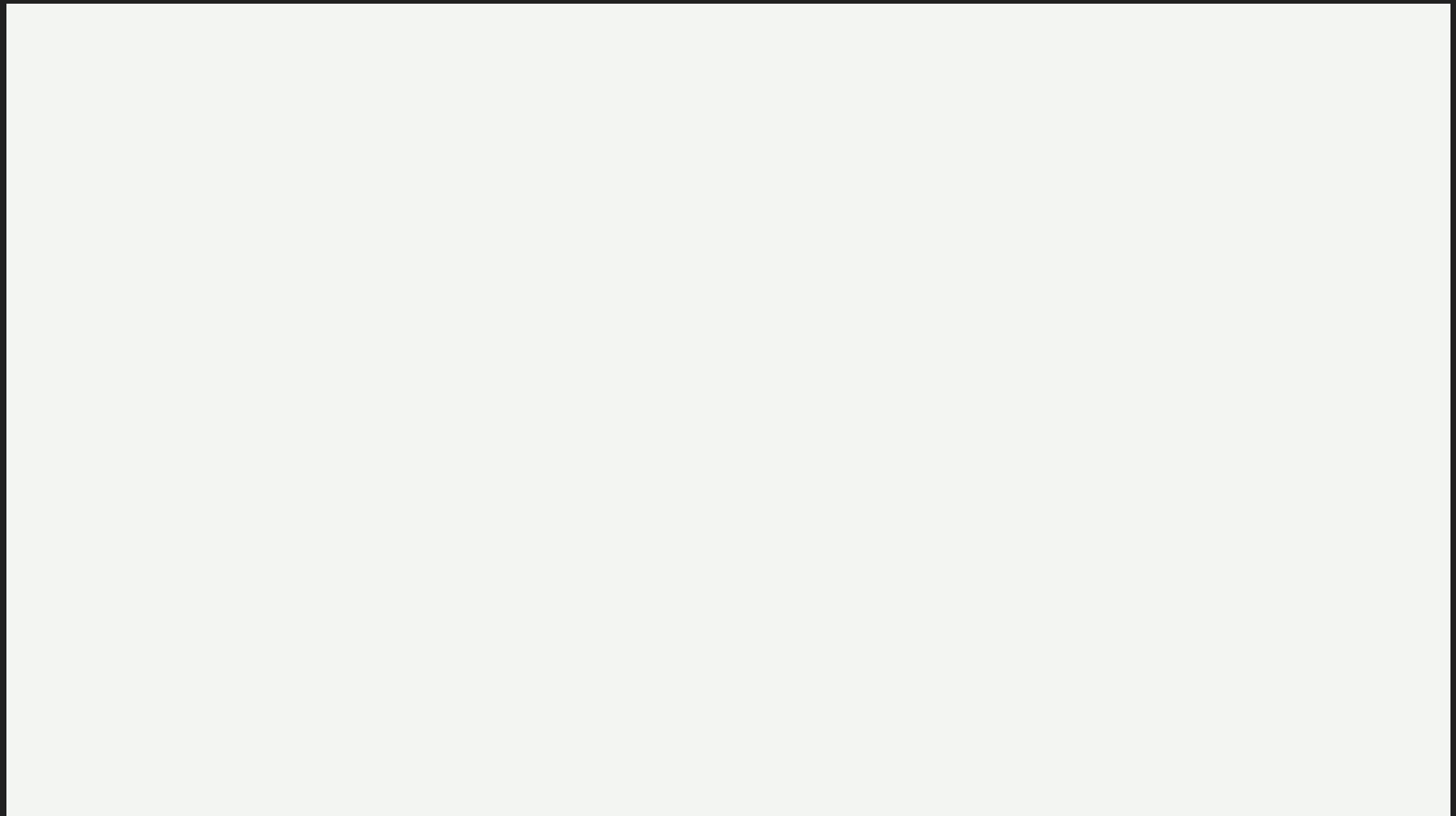


2. Nahziel: RaSTA-Passwort-Angriff

Szenario für den Angriff



Demonstration des bisher Erreichten



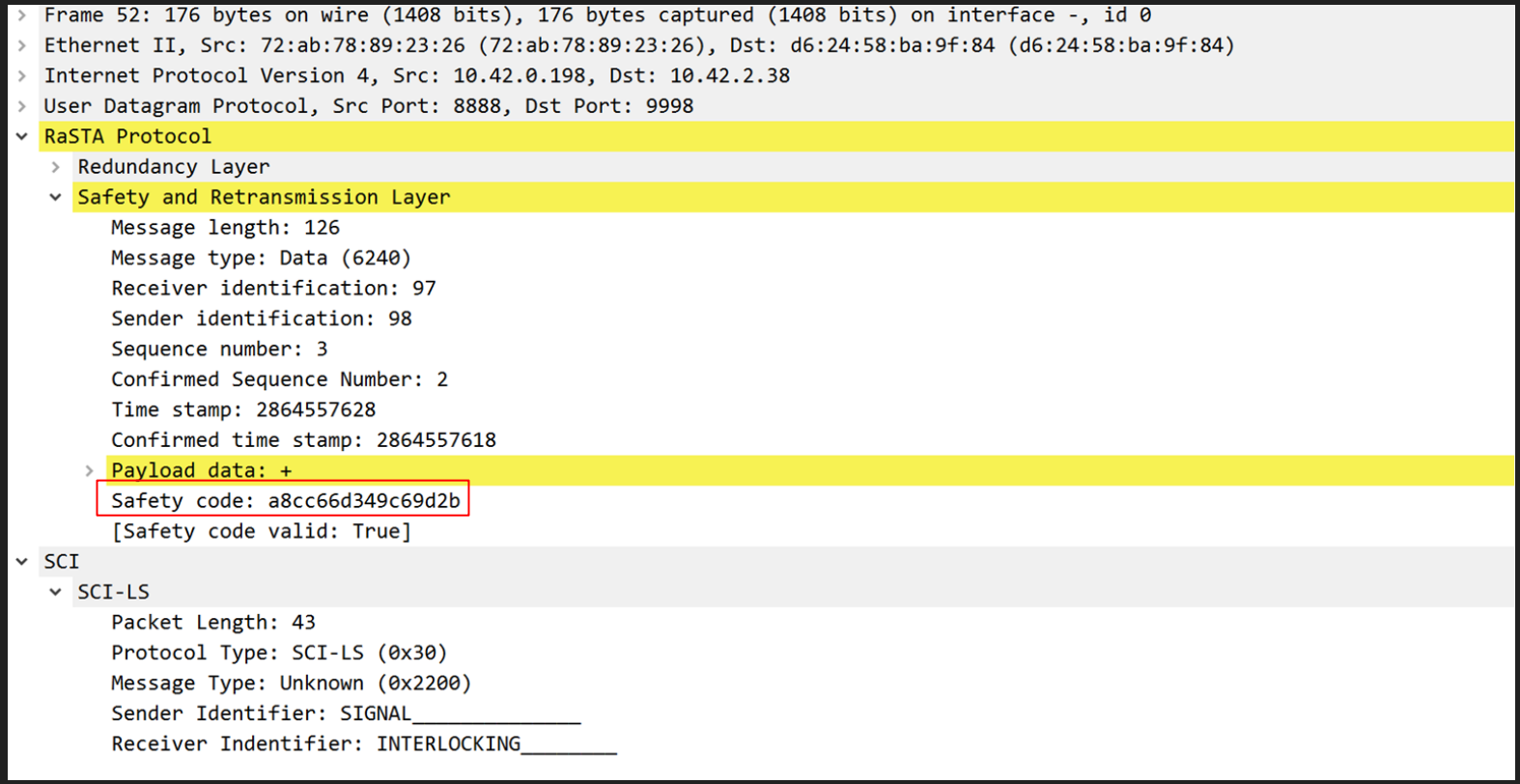
Ziel und TODOs

- aktueller Angriff nimmt Passwort als default / bekannt an
- nächstes Ziel: Brute-Force-Angriff auf aufgezeichneten RaSTA-Traffic

Von Wireshark SVN Tree, GPL,
https://commons.wikimedia.org/w/index.php?curid=1419420

https://hashcat.net/s/i/hashcat-icon.png

Wireshark: Aufzeichnen von RaSTA-Traffic



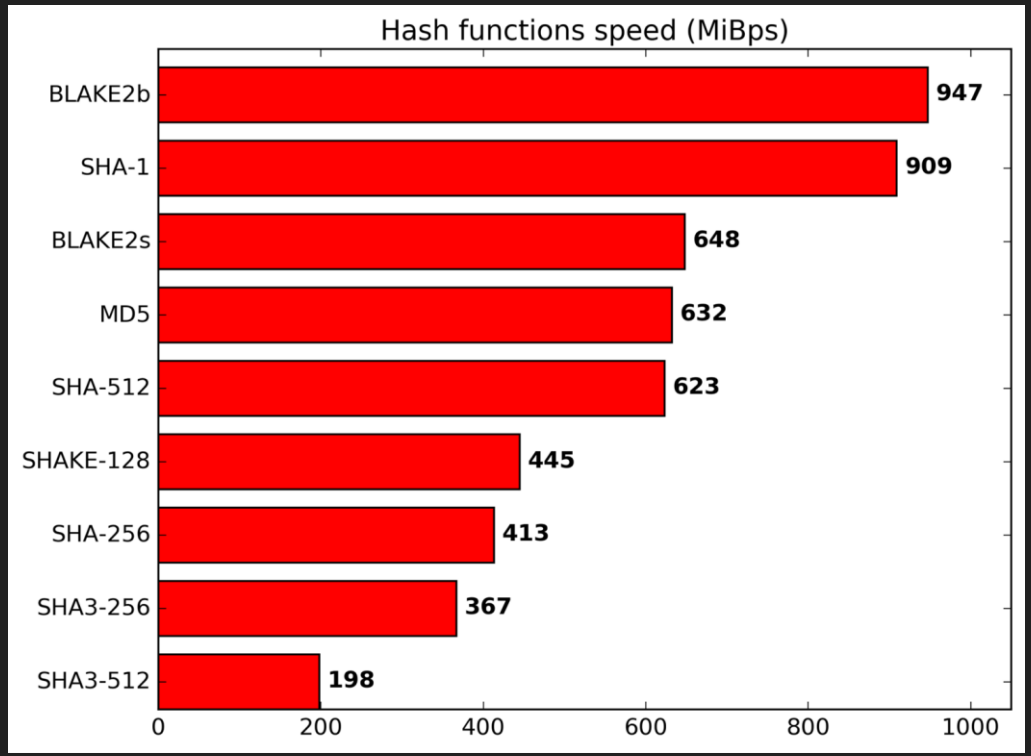
Hashcat: Brute-Force / Wordlist / Regelbasierter Angriff

```
Session..........: hashcat
Status...........: Running
Hash.Mode........: 900 (MD4)
Hash.Target......: a38217d543726545e70685379586f249
Time.Started.....: Mon May 30 12:37:05 2022 (5 mins, 53 secs)
Time.Estimated...: Tue May 31 14:14:06 2022 (1 day, 1 hour)
Kernel.Feature...: Optimized Kernel
Guess.Mask.......: ?a?a?a?a?a?a?a?a [8]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 71935.6 MH/s (20.82ms) @ Accel:256 Loops:1024 Thr:128 Vec:8
Recovered.Total..: 0/1 (0.00%) Digests
Progress.........: 25576361099264/6634204312890625 (0.39%)
Rejected.........: 0/25576361099264 (0.00%)
Restore.Point....: 28639232/7737809375 (0.37%)
Restore.Sub.#1...: Salt:0 Amplifier:677888-678912 Iteration:0-1024
Candidate.Engine.: Device Generator
Candidates.#1....: Q2X-i.,1 -> ujYg7c..
Hardware.Mon.#1..: Temp: 61c Fan:  0% Util: 97% Core:1905MHz Mem:6800MHz Bus:16
```

3. Fernziel: RaSTA-Verbesserung

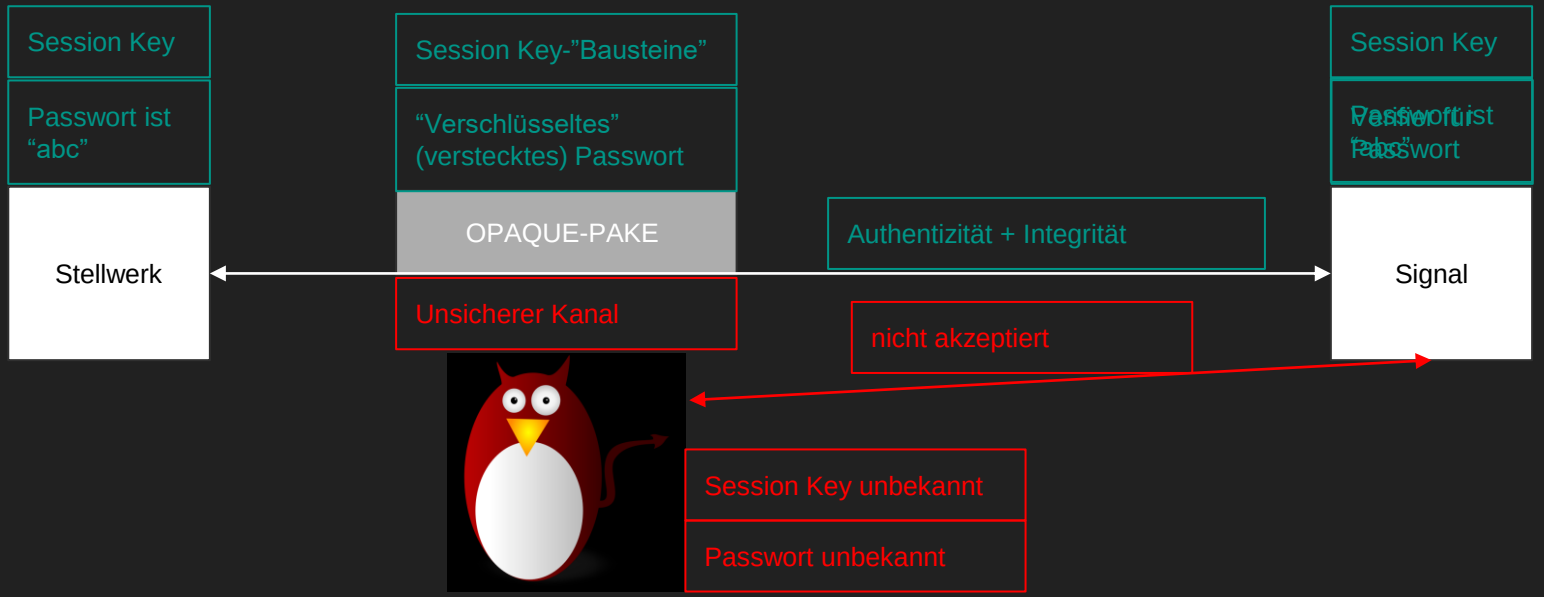
RaSTA Security - Grundproblem

“Security” Performance



https://www.blake2.net/

Wie kann man das Problem umgehen?



Quellen

- Security Analysis of the RaSTA Safety Protocol, TU Darmstadt.
- DIN VDE V 0831-200:2015-06
- RFC 1320
- https://datatracker.ietf.org/meeting/interim-2020-cfrg-01/materials/slides-interim-2020-cfrg-01-sessa-results-of-the-pake-selection-process-00
- Bilder: Public Domain oder eigene Arbeit wenn nicht anders angegeben