

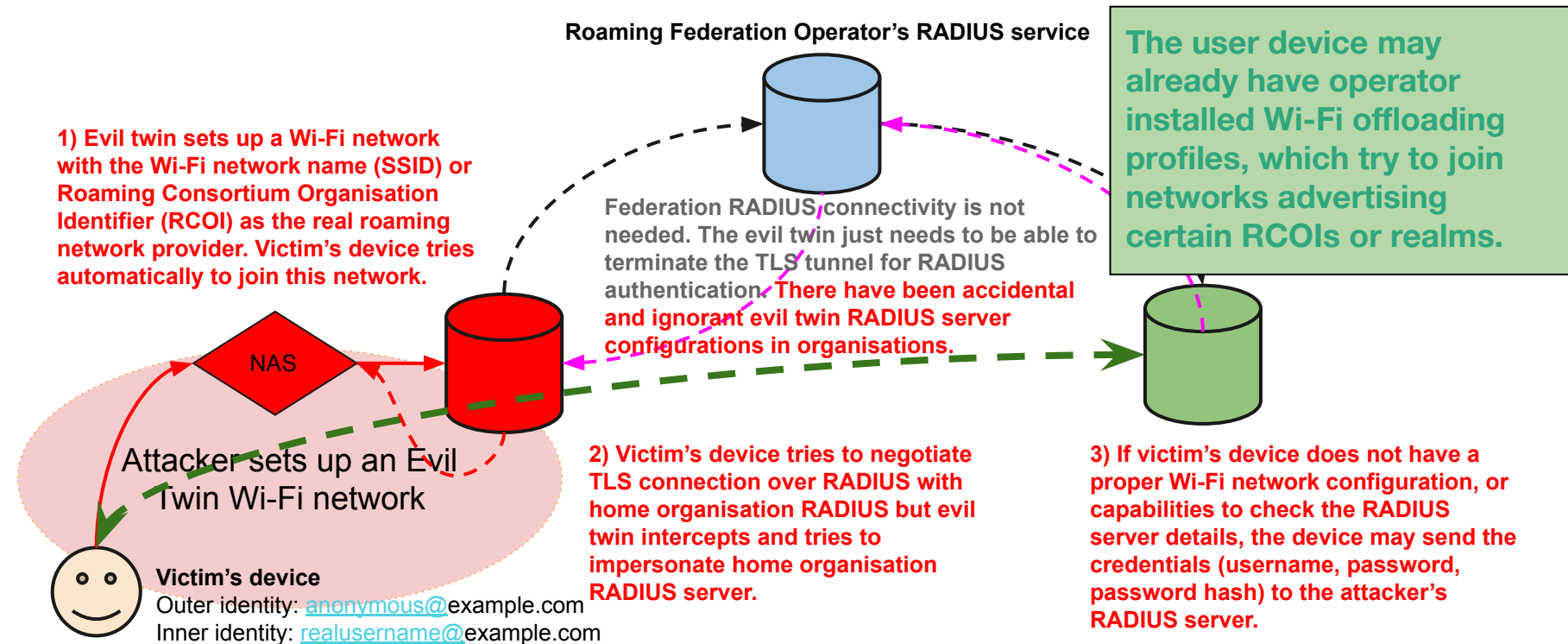
WLPC Prague 2025, 15th of October 2025

Wi-Fi Roaming Security and Privacy

Karri Huhtanen (Radiator Software)

Wi-Fi Roaming Security

Improved evil twin (MitM) attack

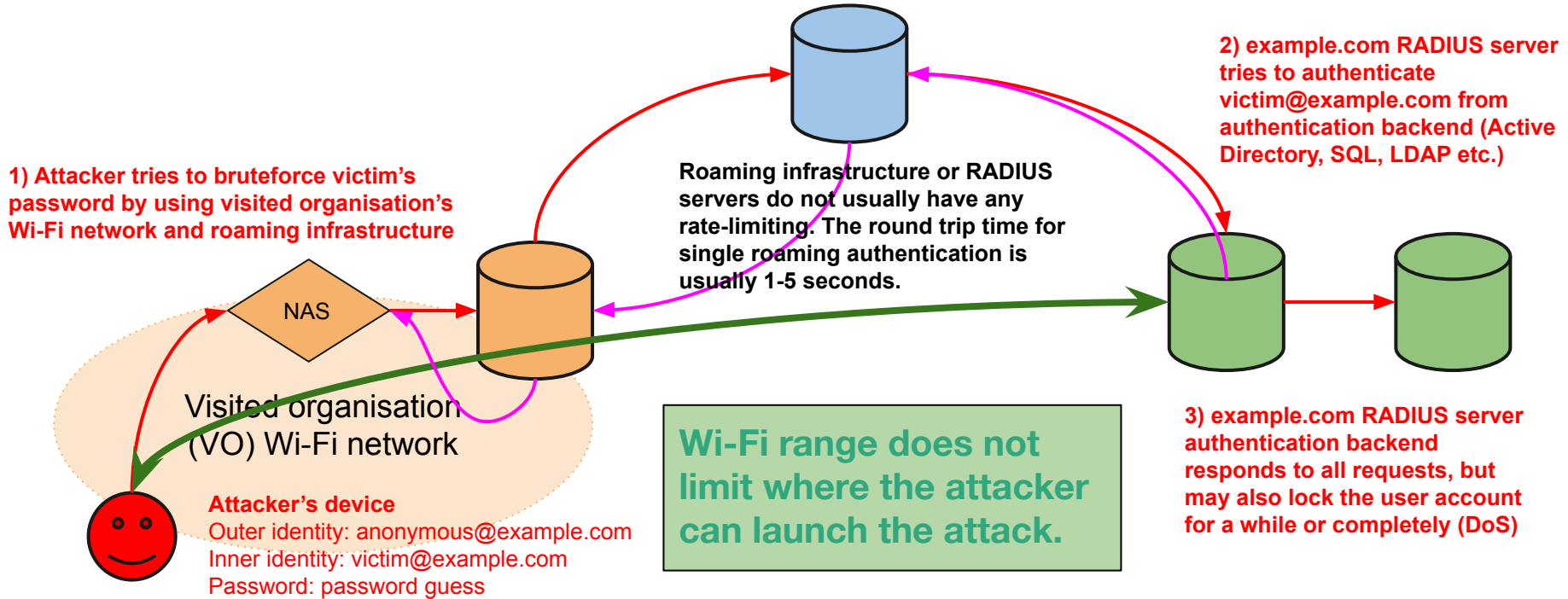


Improved evil twin attack mitigation

- **Proper Wi-Fi configuration profiles** (eduroam-cat/geteduroam.app, Windows policies, Apple Configurator)
- **Using Private CA signed RADIUS server certificate** instead of well-known or system CA (Android) signed one => impersonation with another certificate signed by the same CA does not work (some devices cannot check the certificate CN or SubjectAltNames)
- **Using client-certificate authentication (EAP-TLS) or EAP-PWD** => no credentials sent, but identity may be still sent
- **Rogue access point detection and isolation** features in Wi-Fi controllers
- **Using separate network credentials** (different username and password) or Multi-Factor Authentication => lost credentials are less valuable or do not work



Remote brute-force / Denial of Service (DoS) attack

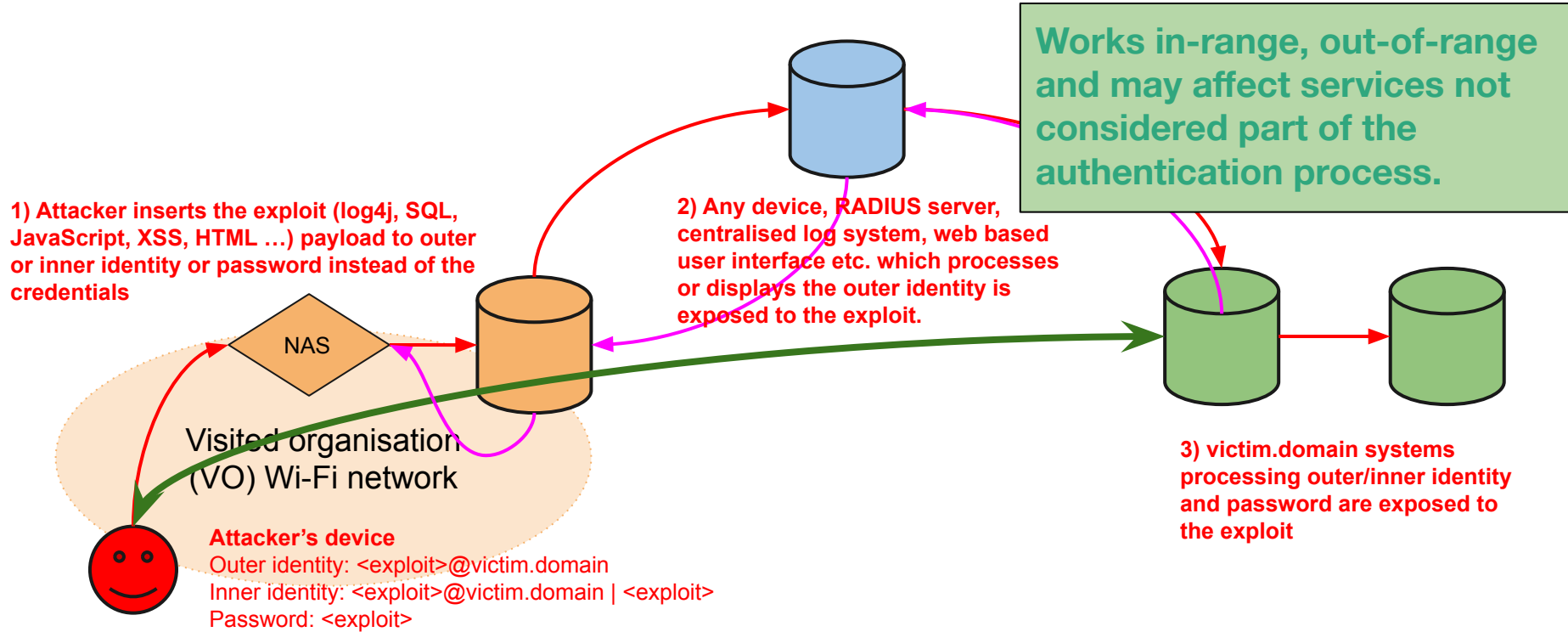


Brute force / Denial of Service (DoS) mitigation

- **Rate limiting RADIUS requests in the home organisation RADIUS server**
 - Can be complex to design, implement and configure depending on the EAP protocol and inner EAP authentication method
 - Contributes to Denial of Service attack
- **Rate limiting requests the in home organisation authentication backend**
 - Backends may not have support for rate limiting
 - Contributes to Denial of Service attack
- **Rate limiting in the Wi-Fi network controller or Visited Organisation RADIUS server**
 - Some support exists for detecting devices failing multiple authentication requests in the controllers
- Automatic locking and unlocking of the user account
- **Rate limiting is rarely done** because real attacks are equally rare



Injection attack via roaming hierarchy



Injection attack comments and mitigation

Comments

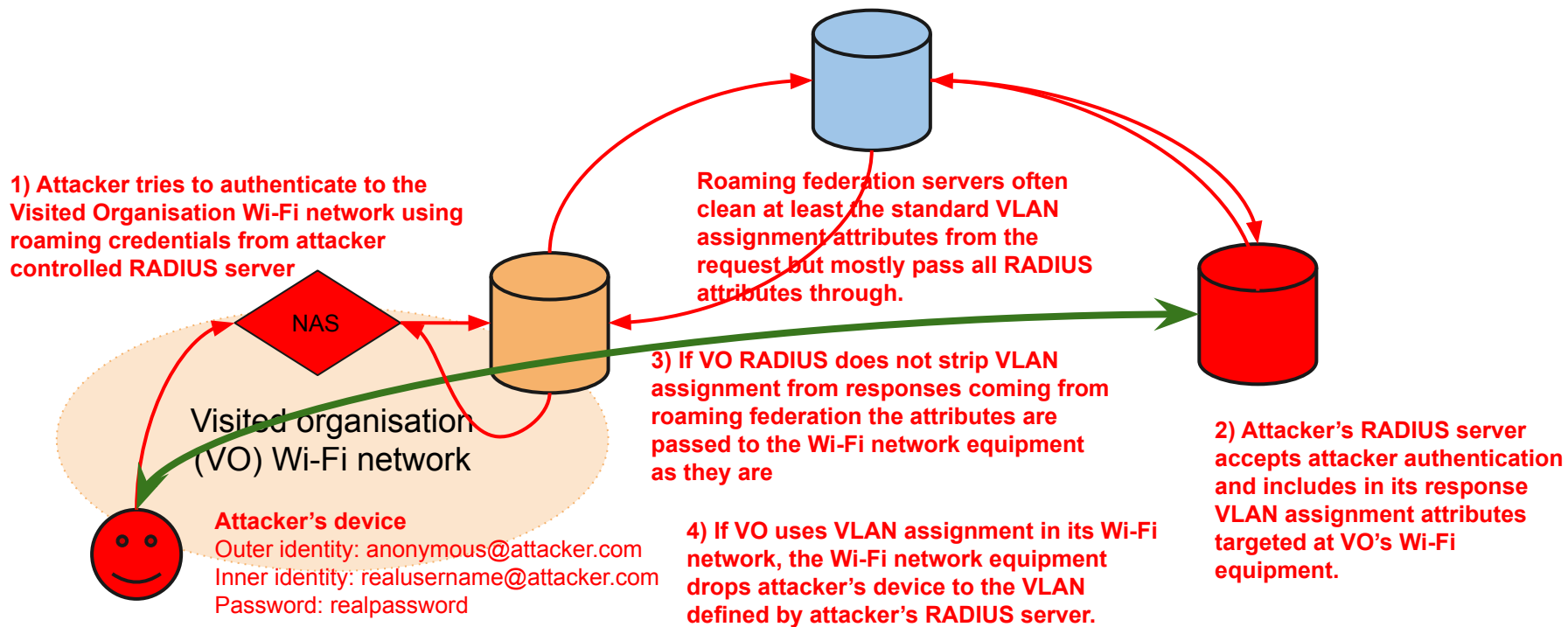
- There have not yet been successful public cases or occurrences of this attack
- In eduroam this was tested when log4j exploit was published but just placing log4j exploit in the RADIUS request did not work
- Maximum length of an RADIUS attribute is 253 characters, which limits exploits

Mitigation

- **Sanitising inputs in software**
- **Sanitising User-Name (outer identity), inner identity and password in RADIUS servers**
 - Done sometimes for example for whitespaces in User-Name
 - Done also sometimes for specific characters, but extra care needs to be taken to not break legit requests
 - Only home organisation is exposed to the exploit placed in the inner identity or password



VLAN hopping / discovery attack



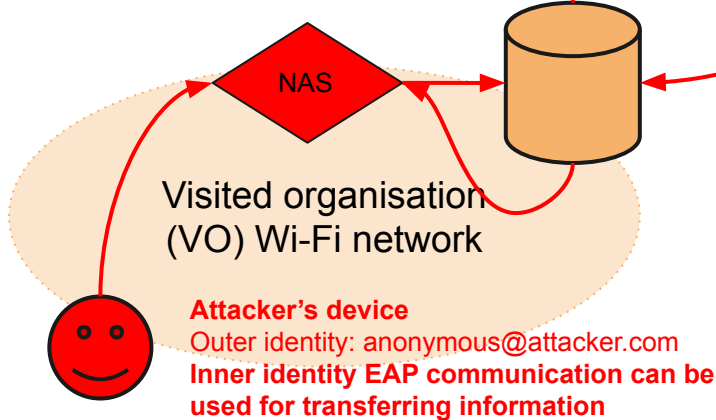
VLAN hopping / discovery attack mitigation

- **Strip standard and vendor specific VLAN assignment RADIUS attributes in the own organisation RADIUS server**
- **Strip attributes in the other federation RADIUS servers**
- **Take care what organisations can join the roaming federation and in identifying them**

Hidden channel communication via roaming

The amount of messages for EAP authentication is not limited. Multiple messages can be sent through roaming federation without ever really reaching authentication decision.

Unsuccessful interrupted EAP authentication may not be logged in the RADIUS servers in between.



Hidden channel communication prevention

- It is unknown if roaming federations have ever been used for this, could hide in the noise of normal authentications
- Requires the attacker organisation to be part of the roaming federation
- Technical prevention is not feasible
- Most efficient mitigation is **taking care what organisations can join the roaming federation and in identifying them**

TLS, PKI and certificates are still hard

- RADIUS over TLS (RadSec) is configured as well or bad as other TLS connections
- RadSec implementations in network vendor devices often do not do proper certificate verification
- Combined with PKI changes and DNS discovery such as in OpenRoaming broken configurations are often possible



Wi-Fi Roaming Privacy

MAC address randomisation, does it really work?

- In most devices **randomised MAC address only changes when a network or profile is deleted and created again**
- In **authenticated and roaming networks MAC address does not really matter**
- **User-Name** and **Chargeable-User-Identity** are **sent in clear text**
 - EAP-TLS with TLS<1.3, PEAP/EAP-TTLS, EAP-SIM / EAP-AKA / EAP-AKA' without IMSI Privacy
- **Outer identity, RADIUS attributes** and **RADIUS accounting** are sent **in clear text** if not protected by IPSEC or RadSec connections.



RADIUS Accounting Information

```
e86bff00 Thu Feb 23 14:50:10 2023 594131: DEBUG: Packet dump:
e86bff00 *** Received from 10.255.255.245 port 61503 ....
e86bff00 Code: Accounting-Request
e86bff00 Identifier: 1
e86bff00 Authentic: <167>[<8>i+<250><208><242><12>A<179><226>d<183><183>S
e86bff00 Attributes:
```

```
e86bff00 Acct-Status-Type = Start
e86bff00 NAS-IP-Address = 10.255.255.245
e86bff00 User-Name = "0001012014020013@wlan.mnc001.mcc001.3gppnetwork.org"
e86bff00 NAS-Port = 0
e86bff00 NAS-Port-Type = Wireless-IEEE-802-11
e86bff00 Calling-Station-Id = "aa2b0b553528"
e86bff00 Called-Station-Id = "6026efcdcdc4"
e86bff00 Framed-IP-Address = 172.16.145.111
e86bff00 Acct-Multi-Session-Id = "AA2B0B553528-1677156607"
e86bff00 Acct-Session-Id = "6026EF5CDC55-AA2B0B553528-63F76102-8F448"
e86bff00 Acct-Delay-Time = 0
e86bff00 Aruba-Essid-Name = "RS-TEST"
e86bff00 Aruba-Location-Id = "rs-aruba-ap-1"
e86bff00 Aruba-User-Vlan = 145
e86bff00 Aruba-User-Role = "RS-TEST"
e86bff00 Aruba-Device-Type = "NOFP"
e86bff00 Acct-Authentic = RADIUS
e86bff00 Service-Type = Login-User
e86bff00 NAS-Identifier = "rs-aruba-ap-1"
e86bff00
```

```
"Chargeable-User-Identity-Request": "66663533393364636265633036636433363230333332633539363730633332633936363935636331353335656332626466396135303336653730393965306563",
```

```
"Framed-IPv6-Address": [
  "fe80::1405:13ff:fe02:5c30",
  "2001:998:1c:2a91:1405:13ff:fe02:5c30",
  "2001:998:1c:2a91:a6d0:fb2d:be31:c46f"
],
```

```
"cisco-avpair": [
  "dc-profile-name=Linux-Workstation",
  "dc-device-name=Unknown Device",
  "dc-device-class-tag=Workstation:Linux-Workstation",
  "dc-certainty-metric=10",
  "dc-opaque=\u0002\u0000\u0000\u0000\u0001\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000\u0000",
  "dc-protocol-map=33",
  "http-tlv=\u0000\u0001\u00000hMozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.32 Safari/537.36",
  "audit-session-id=F7FFFF0A000179F139DC6B16",
  "vlan-id=145",
  "method=dot1x",
  "cisco-wlan-ssid=roam.fi",
  "wlan-profile-name=roam.fi"
],
```



Radiator

How to protect privacy?

- **Use MAC address randomisation**, it makes tracking harder
- **Use anonymous outer identity** in Wi-Fi configurations
- **Don't send RADIUS accounting** if it is not required (eduroam recommendation)
- **Use RadSec** (RADIUS over TLS, RFC 6614) to protect both authentication and accounting
- **Use EAP-TLS with TLSv1.3** for client certificate authentication because it supports identity protection
- **Use IMSI Privacy Protection** supporting clients, server software and operator for **SIM authentication**



Would you like to see this in slow motion?

Disobey 2024 YouTube video (46 minutes)

<https://www.youtube.com/watch?v=WibYgkgVVBg>



Radiator Software Webinars

<https://radiatorsoftware.com/webinars/>