Wi-Fi Roaming Security and Privacy

Disobey, 16th of February 2024

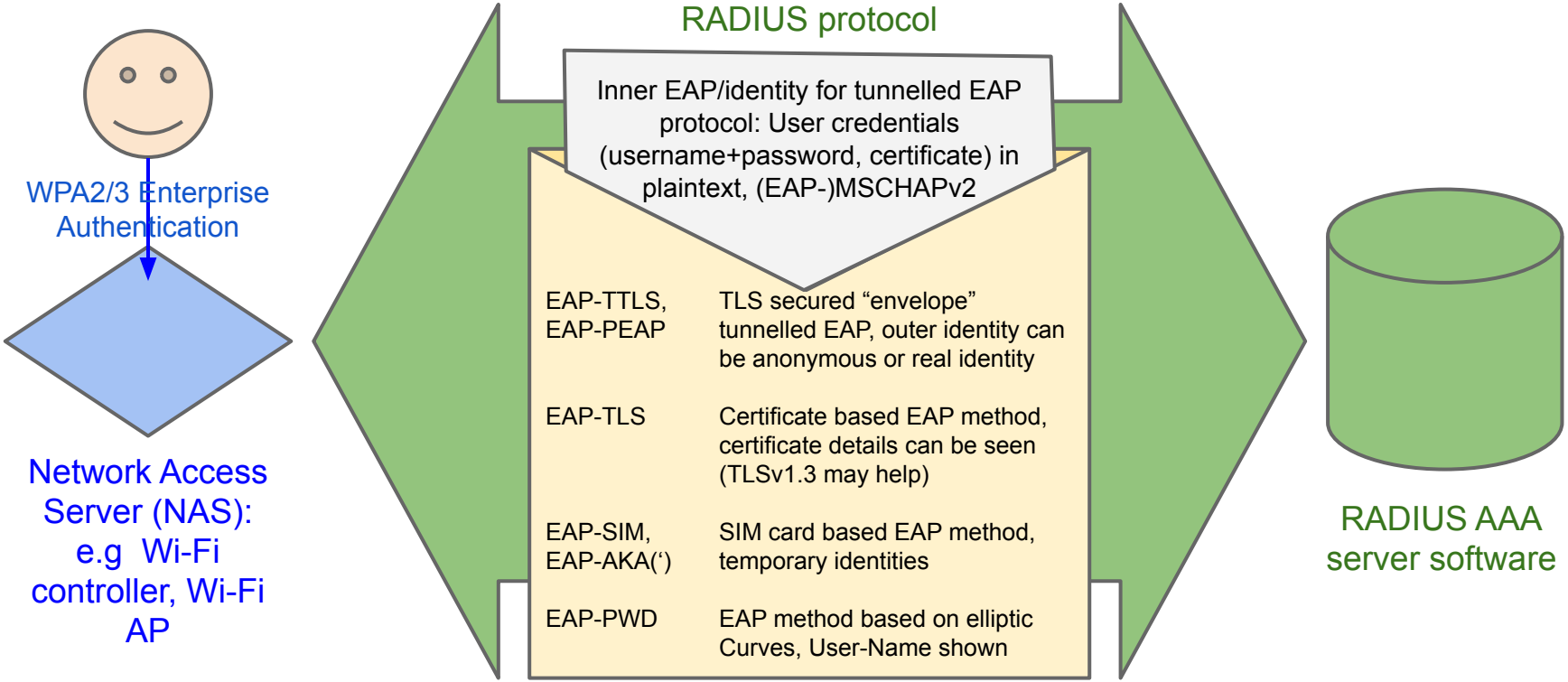
Karri Huhtanen

Background

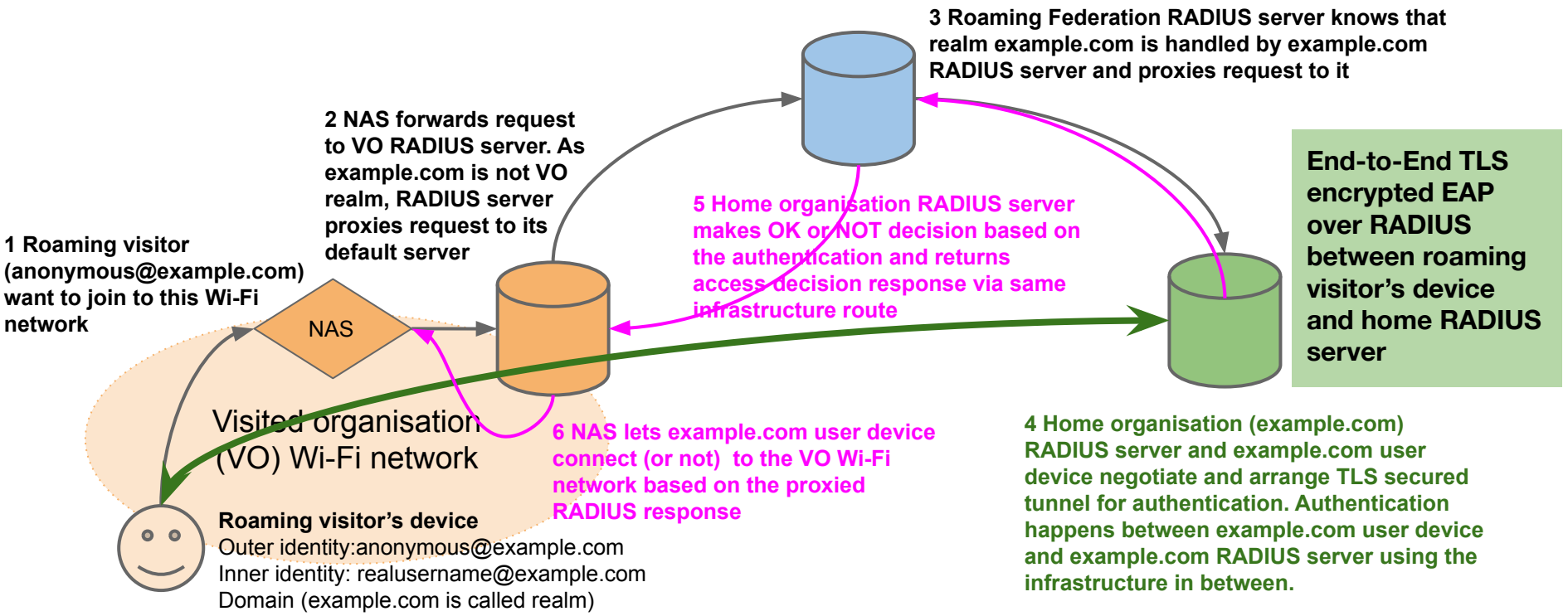
WPA2/3 Enterprise AAA and roaming basics

Radiator

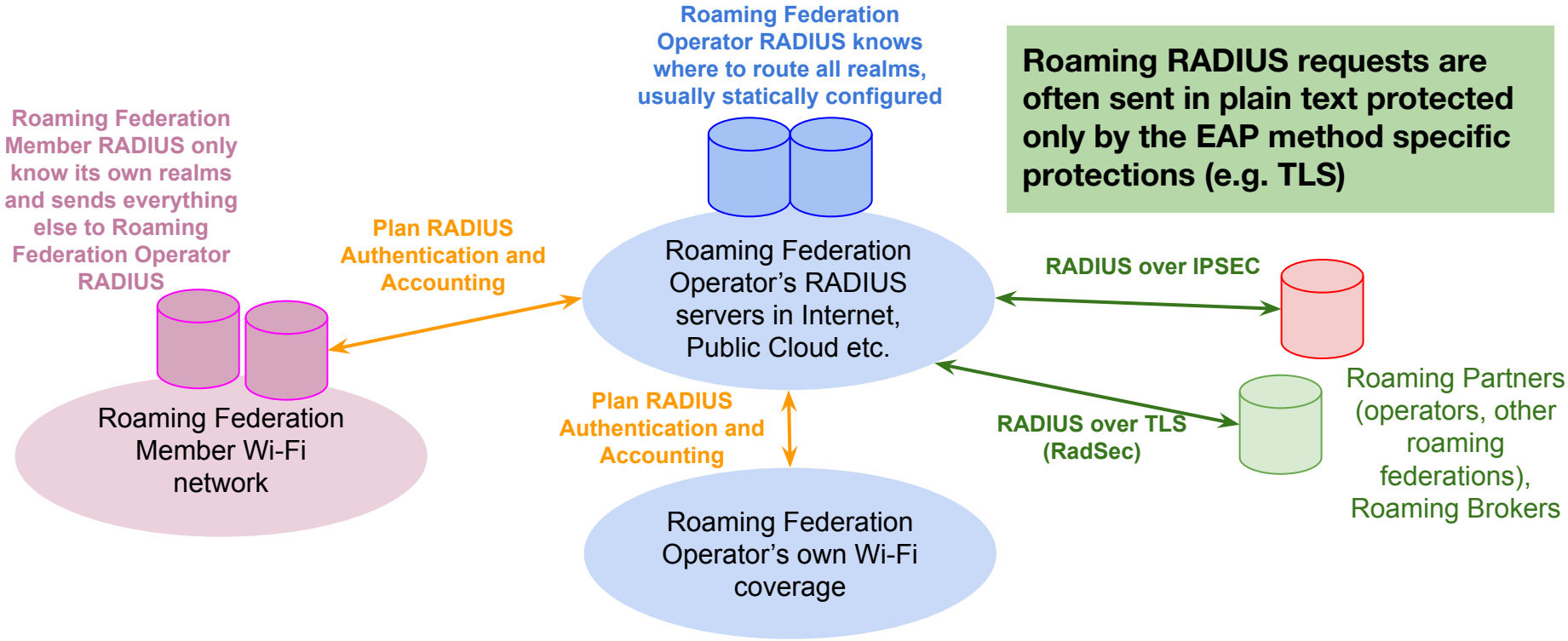
How does WPA2/3 Enterprise AAA work?



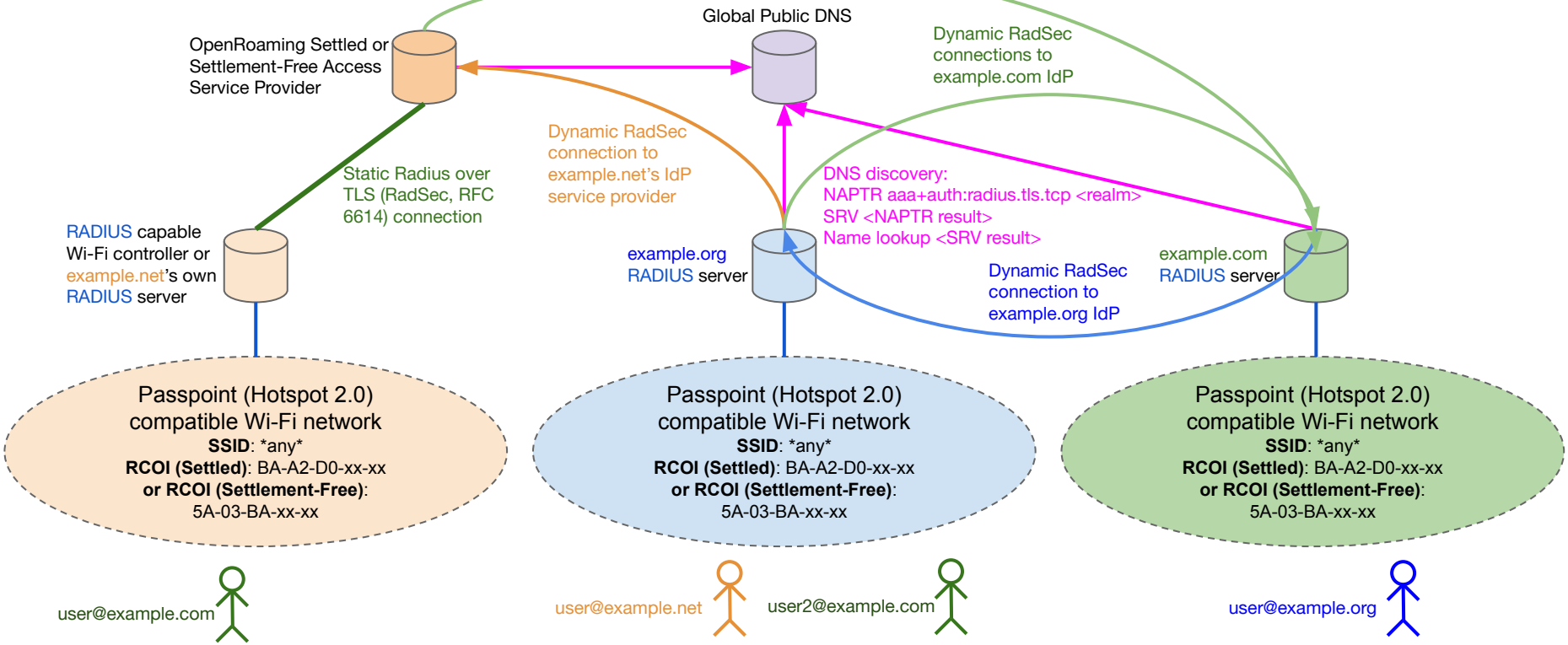
How does Wi-Fi RADIUS roaming work?



Hierarchical RADIUS roaming federation



Peer-to-Peer RADIUS roaming federation



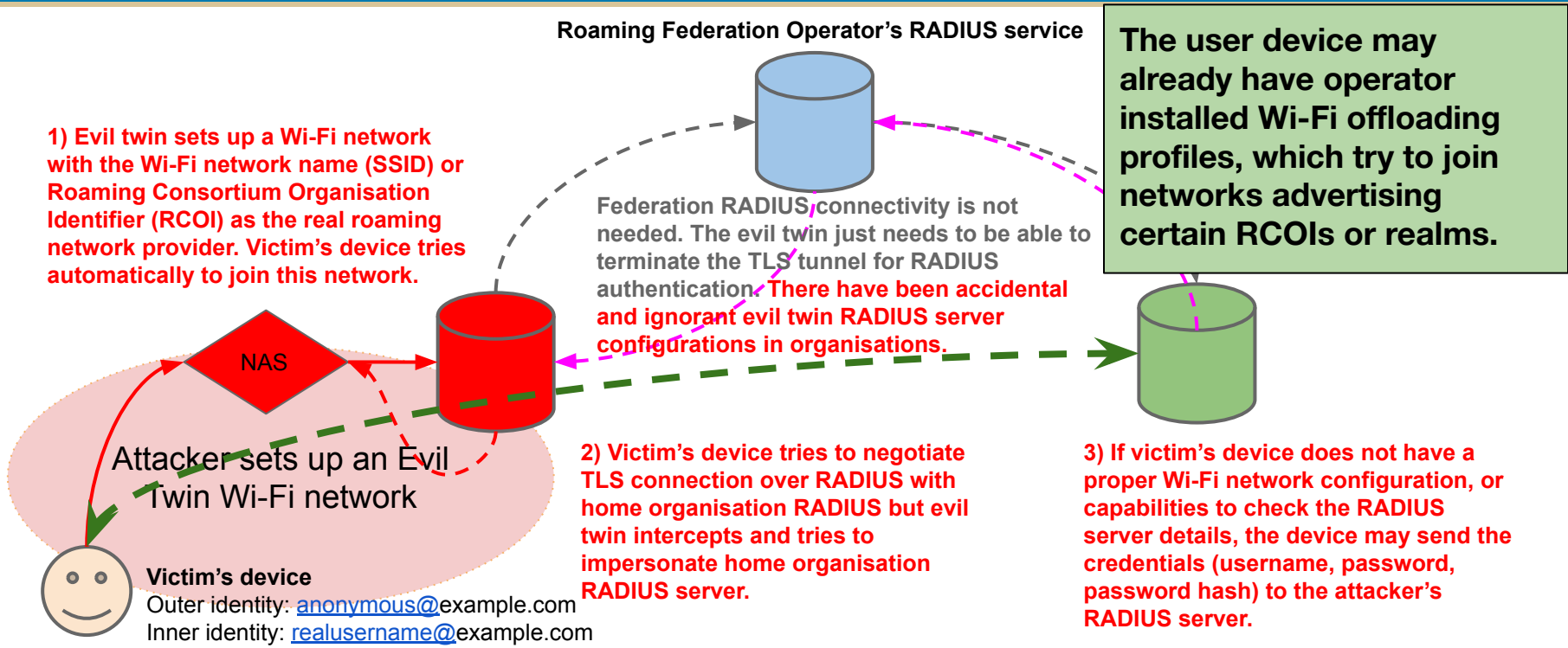
How does Peer-to-Peer Roaming work?

- **Wi-Fi network advertises Roaming Consortium Organisation Id (RCOI)** or **Realm(s)** in beacon messages to get devices **with (pre)installed profiles** to **join automatically**.
- Visited Organisation RADIUS finds a roaming user's home RADIUS service for **with DNS NAPTR/SRV discovery**
- **Dynamic RADIUS over TLS over TCP** connection is authenticated by **roaming federation PKI issued certificates**.

Wi-Fi Roaming Security

Radiator

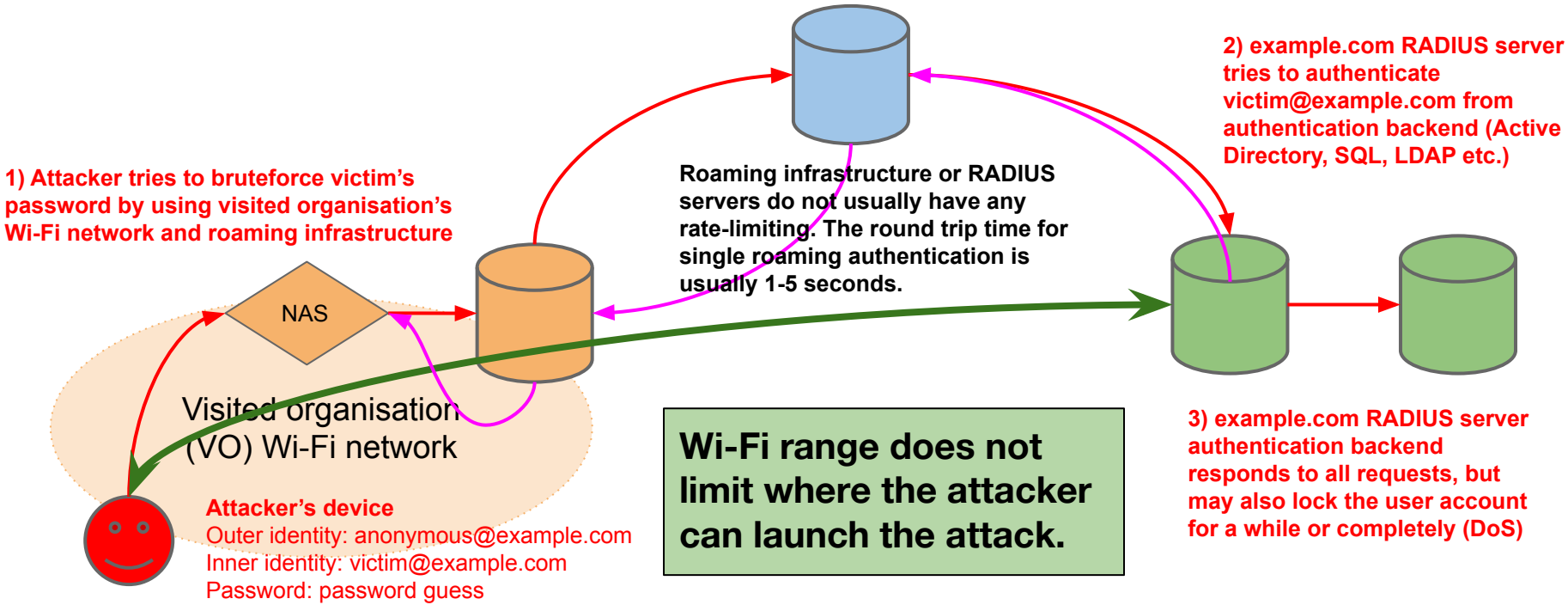
Improved evil twin (MitM) attack



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

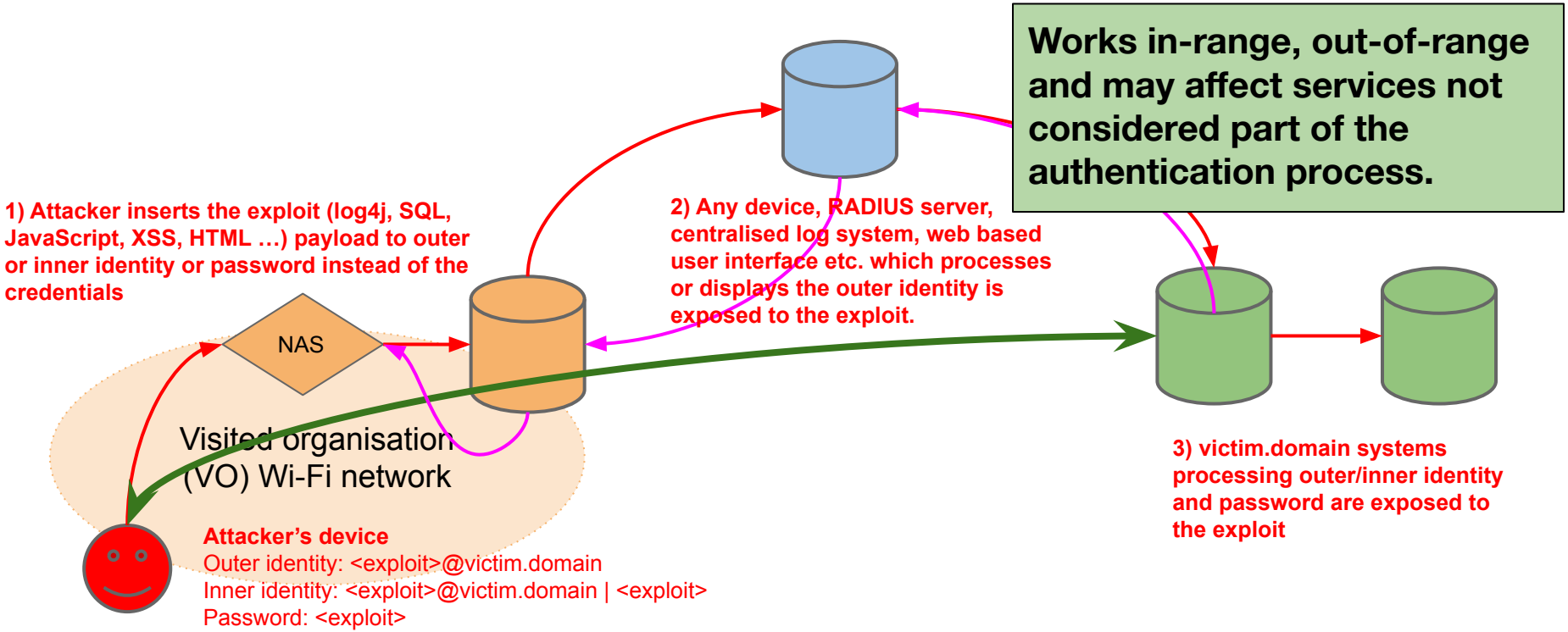
Remote brute-force / Denial of Service (DoS) attack



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

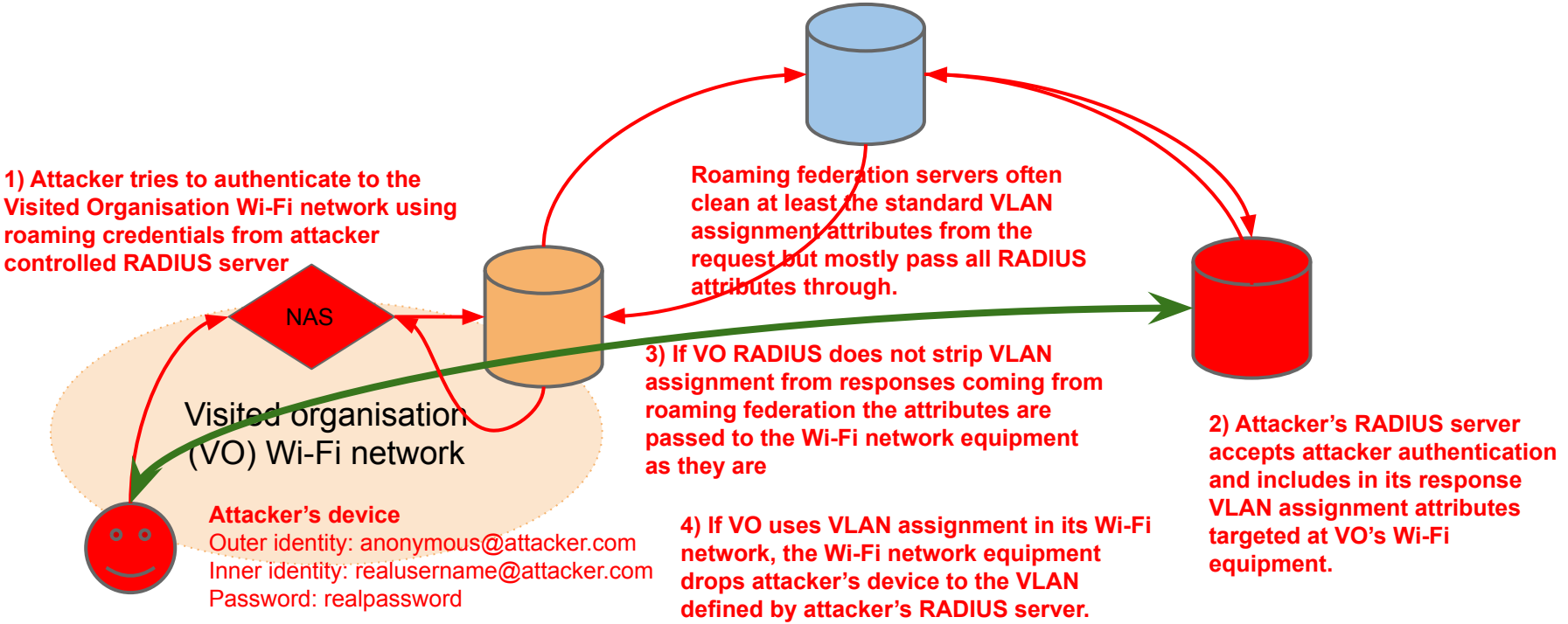
Comments

- **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

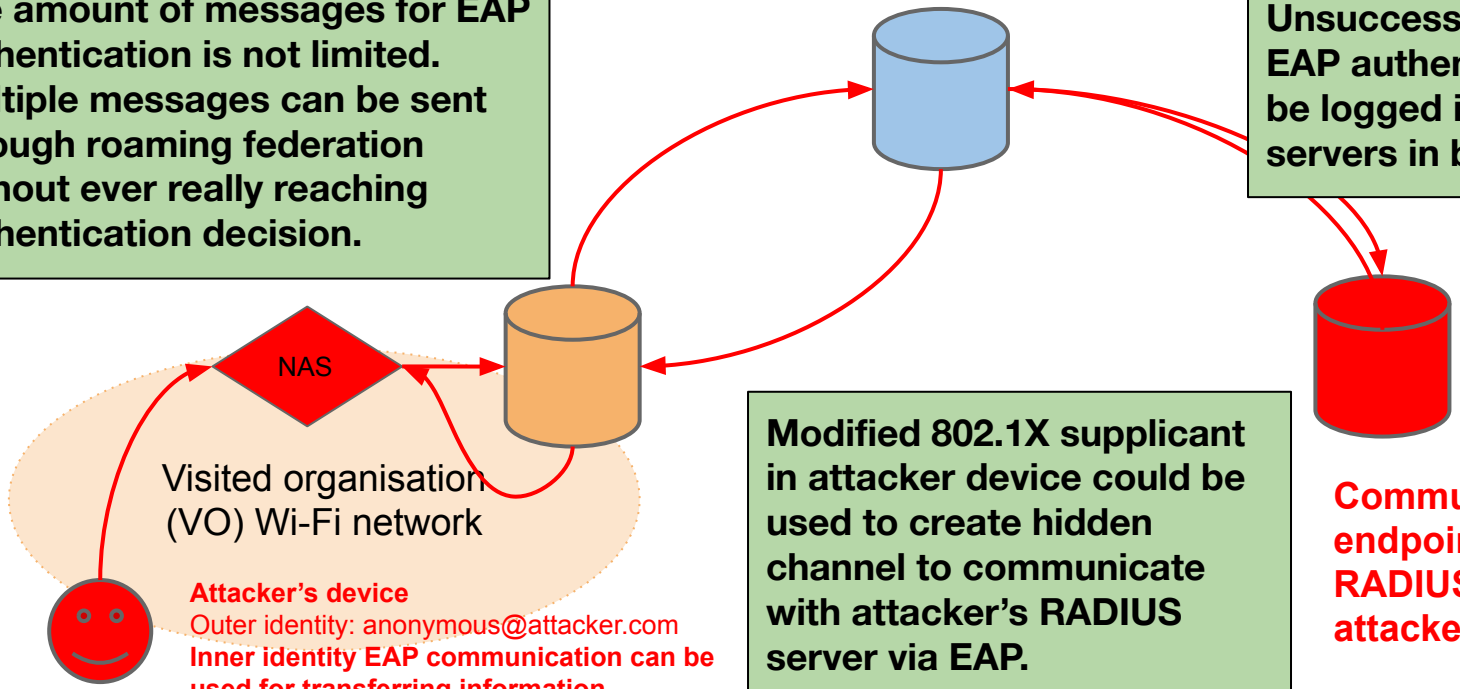


VLAN hopping / discovery attack mitigation

- **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.

Modified 802.1X supplicant in attacker device could be used to create hidden channel to communicate with attacker's RADIUS server via EAP.

Communication endpoint needs to be a RADIUS server under attacker's control.

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**

Wi-Fi Roaming Privacy

Radiator

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 Start message

```
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
```

Note **IMSI in the User-Name, MAC addresses, IP addresses, Session-Ids, Aruba vendor specific RADIUS attributes.**

Modern Wi-Fi APs and controllers also try to identify devices by their 802.1X supplicant, DHCP request parameters, HTTP user agent etc.

RADIUS Accounting Stop message

```
d5b39070 Thu Feb 23 14:53:52 2023 182291: DEBUG: Packet dump:
d5b39070 *** Received from 10.255.255.245 port 61503 ....
d5b39070 Code:       Accounting-Request
d5b39070 Identifier: 1
d5b39070 Authentic:  <188>9>g[<186><157>U|`<244><143>"<171><183><127>
d5b39070 Attributes:
d5b39070       Acct-Status-Type = Stop
d5b39070       NAS-IP-Address = 10.255.255.245
d5b39070       User-Name = "0001012014020013@wlan.mnc001.mcc001.3gppnetwork.org"
d5b39070       NAS-Port = 0
d5b39070       NAS-Port-Type = Wireless-IEEE-802-11
d5b39070       Calling-Station-Id = "aa2b0b553528"
d5b39070       Called-Station-Id = "6026efcdcdc4"
d5b39070       Framed-IP-Address = 172.16.145.111
d5b39070       Acct-Multi-Session-Id = "AA2B0B553528-1677156607"
d5b39070       Acct-Session-Id = "6026EF5CDC55-AA2B0B553528-63F76102-8F448"
d5b39070       Acct-Delay-Time = 0
d5b39070       Aruba-Essid-Name = "RS-TEST"
d5b39070       Aruba-Location-Id = "rs-aruba-ap-1"
d5b39070       Aruba-User-Vlan = 145
d5b39070       Aruba-User-Role = "RS-TEST"
d5b39070       Aruba-Device-Type = "NOFP"
d5b39070       Acct-Input-Octets = 35954
d5b39070       Acct-Output-Octets = 855517
d5b39070       Acct-Input-Packets = 549
d5b39070       Acct-Output-Packets = 453
d5b39070       Acct-Input-Gigawords = 0
```

Note also one Location attribute. There are a lot more related attributes in the standardisation process and under development is also a technology called **Wi-Fi sensing, which probably also brings new attributes to RADIUS requests.**

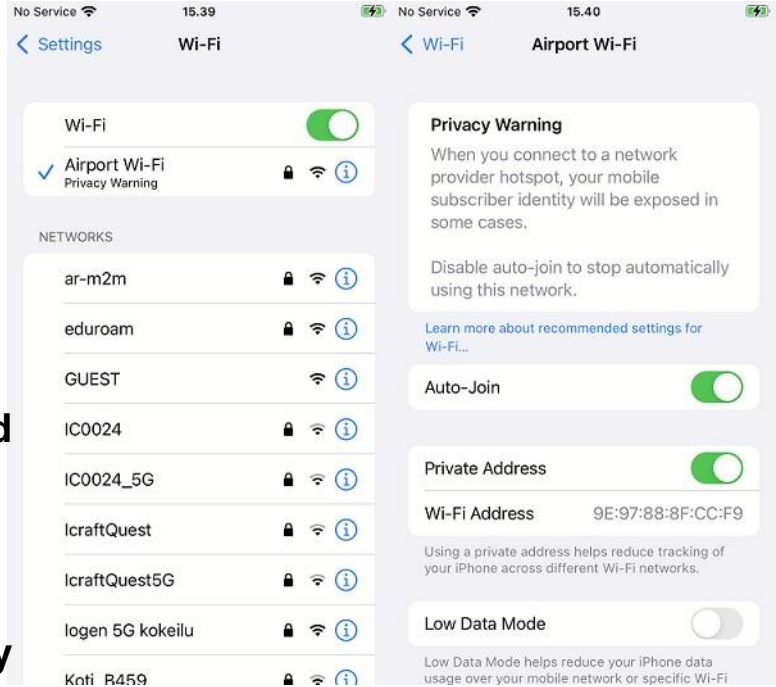
How these attributes are secured and transferred remains to be seen.

Your device may do things you do not know...

- Roaming network profiles make your device try to connect any network advertising suitable network name, roaming consortium organisation ID, realm etc.
- Your device may contain operator profiles not visible or manageable by you
- Even failed attempt to roam to the network may provide trackable information about your device or you.
- Your device may try to join, try to authenticate and then silently fail without alerting you.

EAP-SIM/EAP-AKA/EAP-AKA' privacy

- **EAP-SIM**, **EAP-AKA** and **EAP-AKA'** are **SIM-based WiFi authentication methods** used globally in **Wi-Fi roaming and offloading.**
- On the first connection to a WiFi network, the mobile device **communicates its permanent subscriber identity information (IMSI)**
- **This identity is sent in the clear.**
- a WiFi sniffer can be used **to collect identities and track users**. This tracking can also be done by the venue or network owner when connecting to the WiFi network.
- **IMSI Privacy Protection protects identity already during first authentication**



Example: warning in iOS when joining WiFi without IMSI privacy in place

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**

Ongoing IETF work to improve RADIUS

- **RADIUS EXT**ension (**radext**) group focuses in improving RADIUS:
  - https://datatracker.ietf.org/wg/radext/about/
- **(Datagram) Transport Layer Security ((D)TLS Encryption for RADIUS** updates **RFC6614 (RADIUS/TLS)** and **RFC7360 (RADIUS/DTLS)**
  - https://datatracker.ietf.org/doc/draft-ietf-radext-radiusdtls-bis/
- **Deprecating Insecure Practices in RADIUS** deprecates MD5, CHAP, insecure transports, plain text RADIUS**:**
  - https://datatracker.ietf.org/doc/draft-ietf-radext-deprecating-radius/
- **RADIUS** and **TLS-PSK** describes how TLS-PSK should be used:
  - https://datatracker.ietf.org/doc/draft-ietf-radext-tls-psk/
- Updating old RADIUS with negotiation: **RADIUS ALPN and removing MD5**:
  - https://datatracker.ietf.org/doc/draft-ietf-radext-radiusv11/


Radiator
Thank you!
Questions, comments?
Mastodon: @khuhtanen@infosec.exchange
X: @khuhtanen
SlideShare: https://www.slideshare.net/khuhtanen/presentations

Operating System	Supports Associated MAC Randomization	Default Status	Network Based Per SSID	Time Based
Apple iOS 13	NO			
Apple iPadOS 13	NO			
Apple iOS 14	YES	ENABLED	ENABLED	Possible Future Release
Apple iPadOS 14	YES	ENABLED	ENABLED	Possible Future Release
MacOS 10.15: Catalina	NO			
MacOS 11: Big Sur (*2)	NO			
Android 10	YES	ENABLED	ENABLED	
Android 11	YES	ENABLED	ENABLED	NO (*1)
Windows 10	YES	DISABLED	OPTIONAL	OPTIONAL (24 hours)

*1 - A developer option called 'enhanced MAC Randomization' introduces time based

*2 - Correct at time of publication (macOS 11 is still in BETA phase)

Dated: September 2020

globalreach

@DrCSpencer

Check also globalreachtech.com WWW pages for **more analysis** of **MAC address randomisation** by **Dr Chris Spencer**