Radiator

WiFi Roaming Security and Privacy

23rd and 25th of May 2023

Karri Huhtanen

Radiator

Live Webinars in May and June 2023

Wi-Fi Roaming and Security

23rd of May 2023 (1h): 08:00 UTC, 10:00 CEST

25th of May 2023 (1h): 16:00 UTC, 09:00 PDT, 12:00 EDT

Wi-Fi Roaming Security topics:

Evil Twin Man-in-the-Middle (MitM)

Remote Brute Force / Denial of Service (DoS)

(log4j) Injection

VLAN Penetration/Hopping

Wi-Fi Roaming Privacy topics:

MAC address based tracking

MAC address randomisation

Roaming RADIUS authentication and accounting privacy

SIM authentication privacy and IMSI privacy protection

Radiator, OpenRoaming and IETF update

6th of June 2023 (1h): 08:00 UTC, 10:00 CEST

8th of June 2023 (1h): 16:00 UTC, 09:00 PDT, 12:00 EDT

Webinar topics:

Radiator 4.28 release highlights

Radiator OpenRoaming enhancements

Radiator OpenRoaming Configuration Guide update

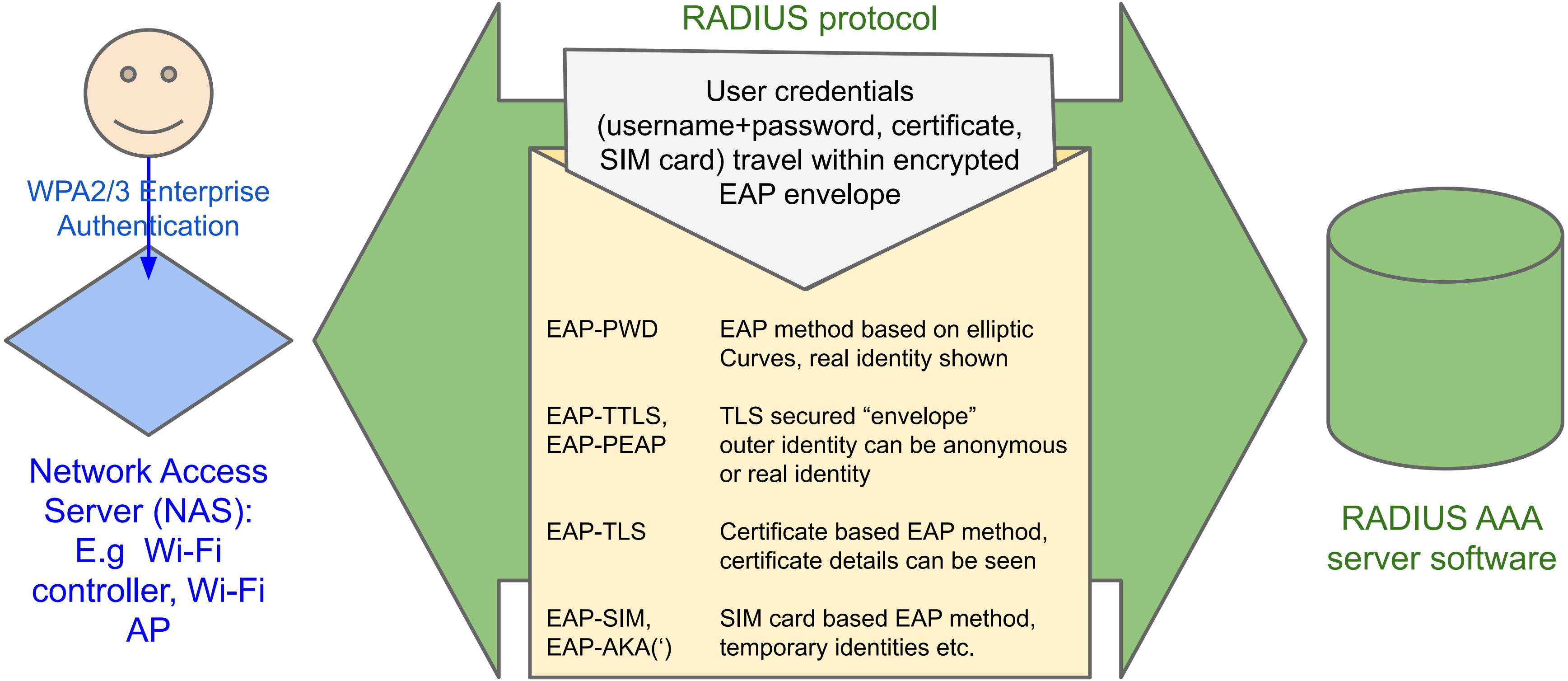
IETF standardisation and Radiator roadmap

Background

about Wi-Fi network security and roaming basics

Radiator

How does WPA2/3 Enterprise AAA work?



WPA2/3 Enterprise Authentication

Network Access Server (NAS): E.g Wi-Fi controller, Wi-Fi AP

RADIUS protocol

User credentials (username+password, certificate, SIM card) travel within encrypted EAP envelope

EAP-PWD	EAP method based on elliptic Curves, real identity shown
EAP-TTLS, EAP-PEAP	TLS secured “envelope” outer identity can be anonymous or real identity
EAP-TLS	Certificate based EAP method, certificate details can be seen
EAP-SIM, EAP-AKA(‘)	SIM card based EAP method, temporary identities etc.

RADIUS AAA server software

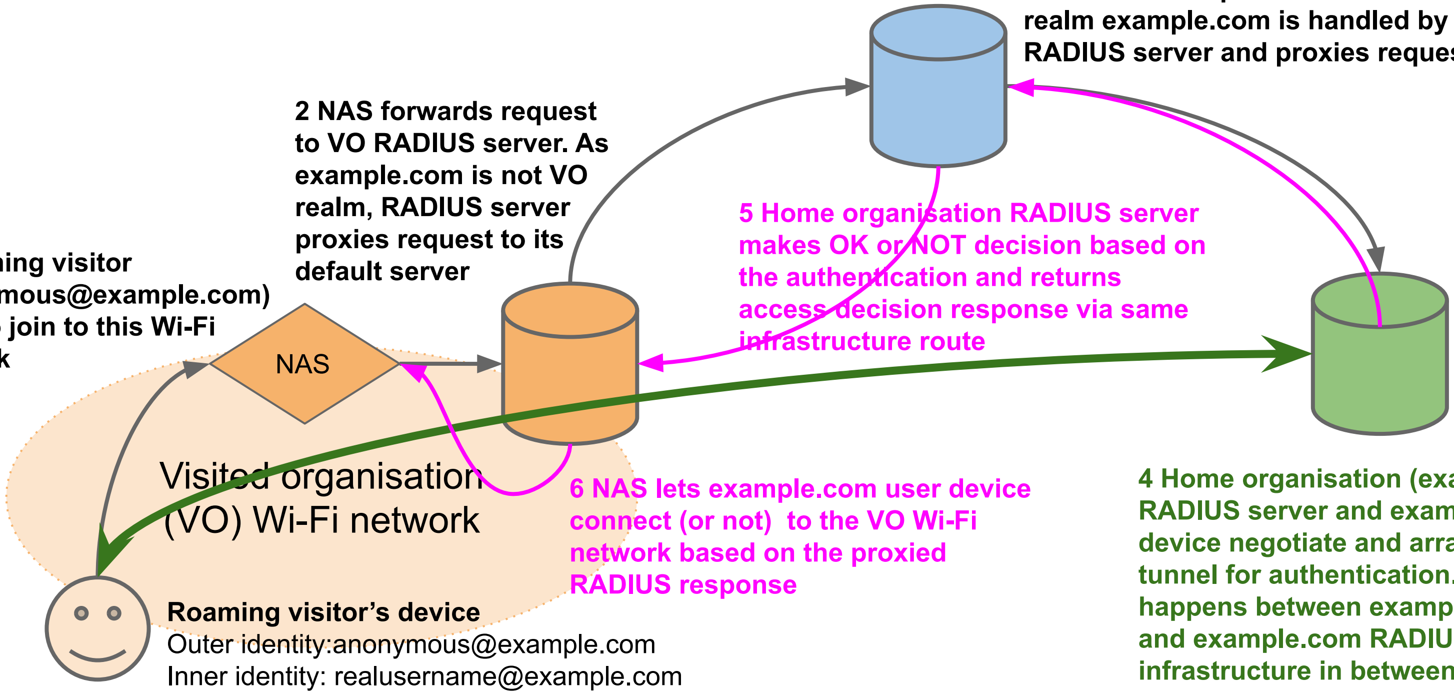
So where does WPA2/3 Enterprise AAA fail?

- **Very rarely** with **technology**
- **Sometimes** with **network and security design**
- **Often** with **misconfiguration** or **lack of configuration provisioning**
- **Most commonly** with **end users** and **manual device configuration**

What is the difference between WPA2 and WPA3?

- WPA3 mandates Protected Management Frames (PMF), WPA2 has those, but by default does not mandate their use
- WPA3 has additional stronger encryption methods, improvements in the key exchange (SAE instead of PSK)
- WPA2 will still be around and can be secured more with mandating PMF and disabling WPA1, TKIP compatibility

How does Wi-Fi RADIUS roaming work?



1 Roaming visitor (anonymous@example.com) want to join to this Wi-Fi network

2 NAS forwards request to VO RADIUS server. As example.com is not VO realm, RADIUS server proxies request to its default server

3 Federation Top Level RADIUS server knows that realm example.com is handled by example.com RADIUS server and proxies request to it

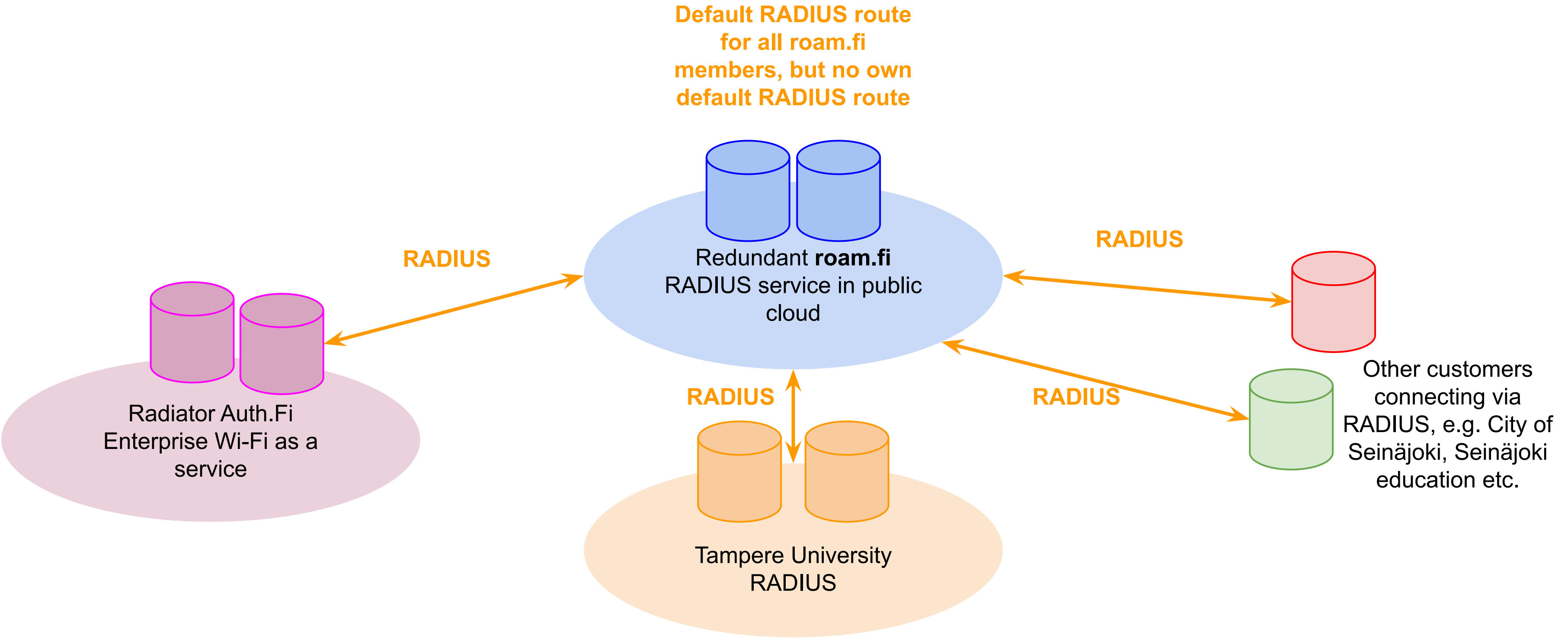
4 Home organisation (example.com) RADIUS server and example.com user device negotiate and arrange TLS secured tunnel for authentication. Authentication happens between example.com user device and example.com RADIUS server using the infrastructure in between.

5 Home organisation RADIUS server makes OK or NOT decision based on the authentication and returns access decision response via same infrastructure route

6 NAS lets example.com user device connect (or not) to the VO Wi-Fi network based on the proxied RADIUS response

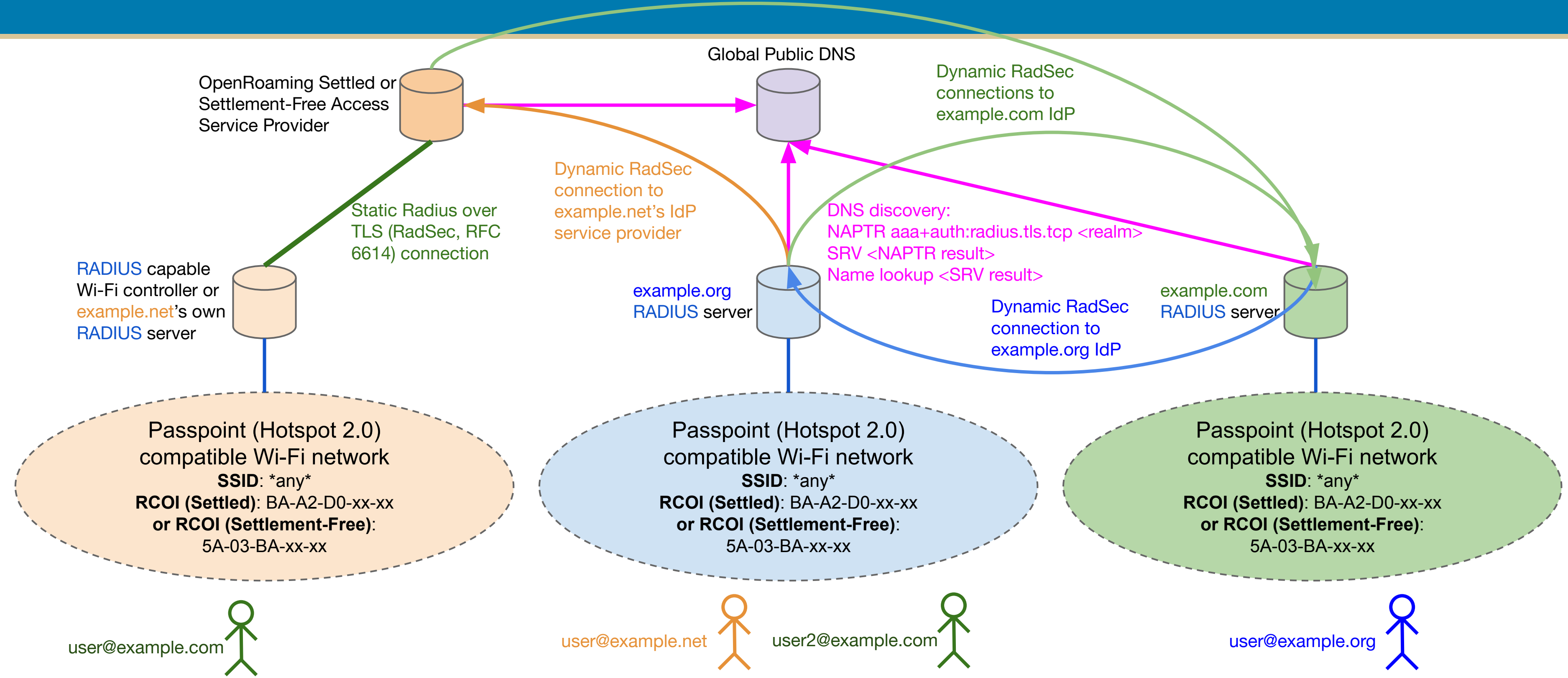
Roaming visitor’s device
Outer identity:anonymous@example.com
Inner identity: realusername@example.com

RADIUS based roaming federation



How does OpenRoaming work?

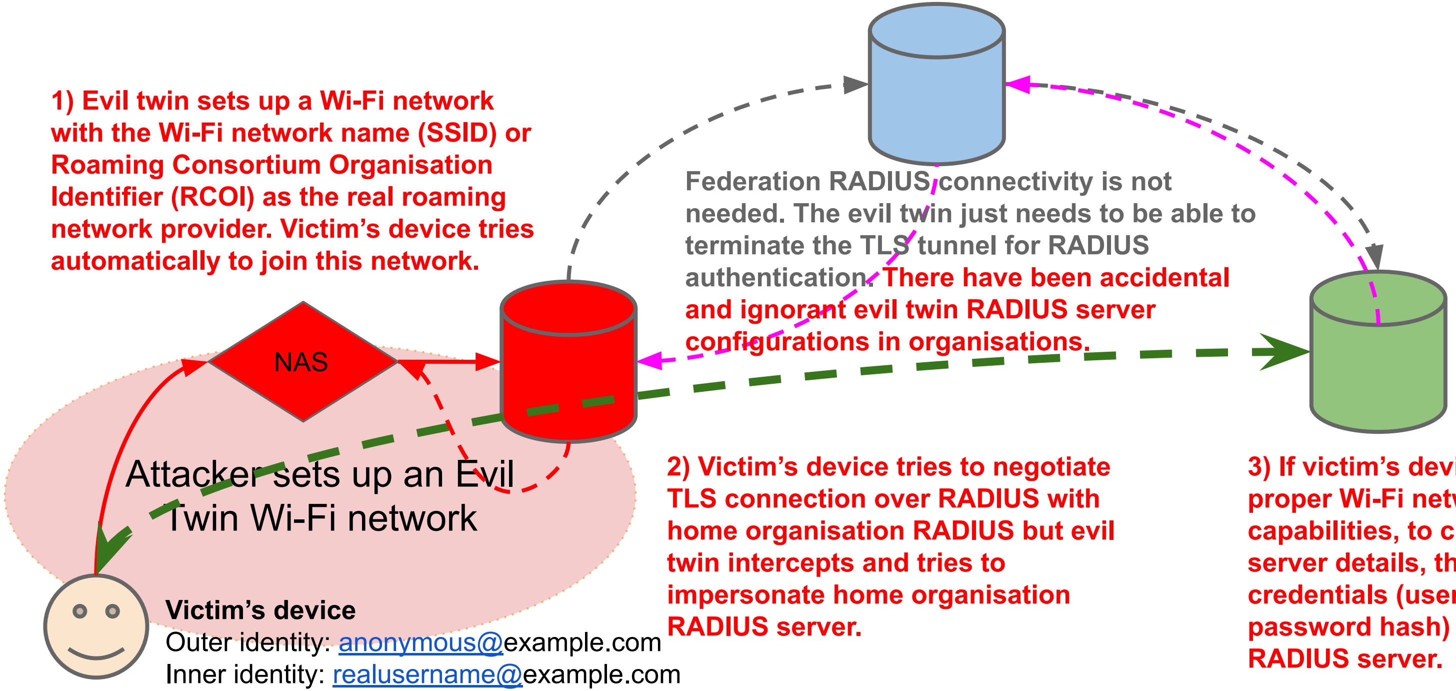
(https://wballiance.com/openroaming/)


Global Public DNS
OpenRoaming Settled or Settlement-Free Access Service Provider
Dynamic RadSec connections to example.com IdP
Dynamic RadSec connection to example.net's IdP service provider
Static Radius over TLS (RadSec, RFC 6614) connection
DNS discovery:
NAPTR aaa+auth:radius.tls.tcp <realm>
SRV <NAPTR result>
Name lookup <SRV result>
RADIUS capable Wi-Fi controller or example.net's own RADIUS server
example.org RADIUS server
Dynamic RadSec connection to example.org IdP
example.com RADIUS server
Passpoint (Hotspot 2.0) compatible Wi-Fi network
SSID: *any*
RCOI (Settled): BA-A2-D0-xx-xx
or RCOI (Settlement-Free):
5A-03-BA-xx-xx
Passpoint (Hotspot 2.0) compatible Wi-Fi network
SSID: *any*
RCOI (Settled): BA-A2-D0-xx-xx
or RCOI (Settlement-Free):
5A-03-BA-xx-xx
Passpoint (Hotspot 2.0) compatible Wi-Fi network
SSID: *any*
RCOI (Settled): BA-A2-D0-xx-xx
or RCOI (Settlement-Free):
5A-03-BA-xx-xx
user@example.com
user@example.net
user2@example.com
user@example.org

Wi-Fi Roaming Security

Radiator

Evil Twin Man-in-the-Middle (MitM) attack



Federation Top Level RADIUS server

1) Evil twin sets up a Wi-Fi network with the Wi-Fi network name (SSID) or Roaming Consortium Organisation Identifier (RCOI) as the real roaming network provider. Victim's device tries automatically to join this network.

Federation RADIUS connectivity is not needed. The evil twin just needs to be able to terminate the TLS tunnel for RADIUS authentication. There have been accidental and ignorant evil twin RADIUS server configurations in organisations.

2) Victim's device tries to negotiate TLS connection over RADIUS with home organisation RADIUS but evil twin intercepts and tries to impersonate home organisation RADIUS server.

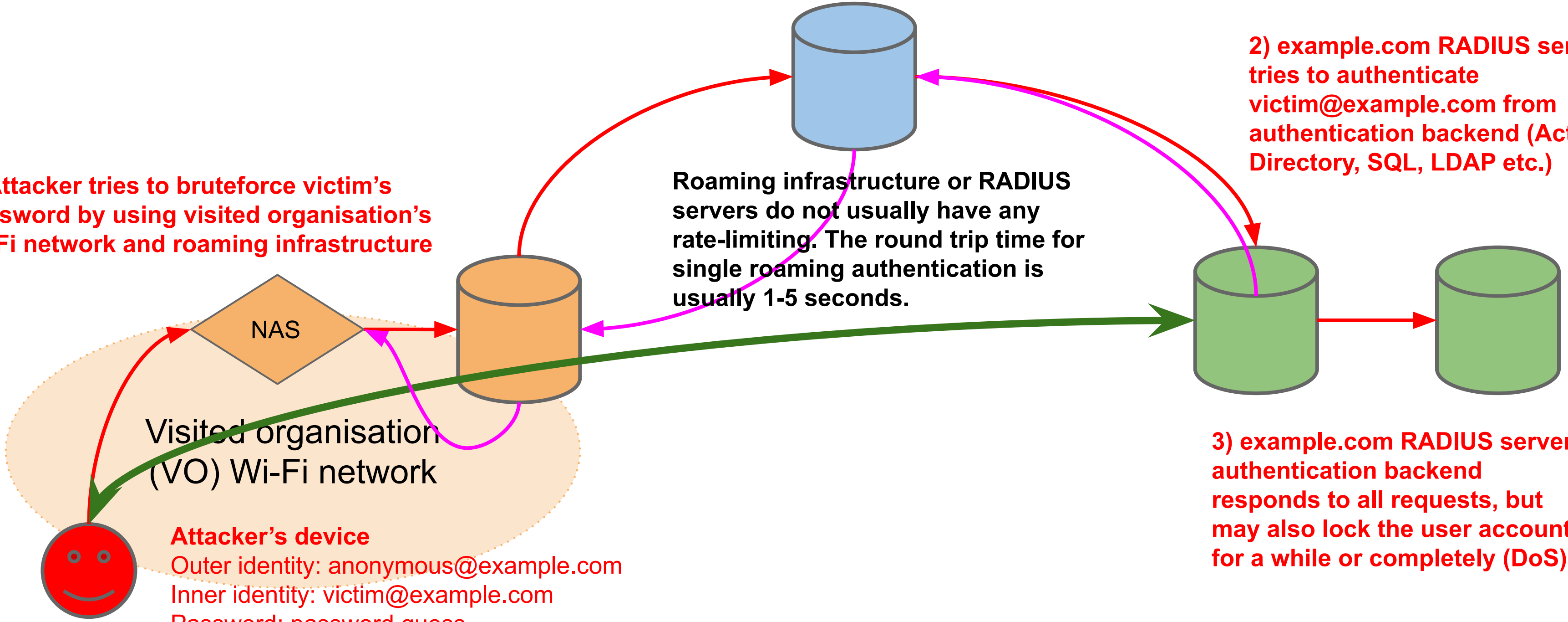
3) If victim's device does not have a proper Wi-Fi network configuration, or capabilities, to check the RADIUS server details, the device may send the credentials (username, password, password hash) to the attacker's RADIUS server.

Victim's device
Outer identity: anonymous@example.com
Inner identity: realusername@example.com

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

Brute force / Denial of Service (DoS) attack



1) Attacker tries to bruteforce victim’s password by using visited organisation’s Wi-Fi network and roaming infrastructure

Roaming infrastructure or RADIUS servers do not usually have any rate-limiting. The round trip time for single roaming authentication is usually 1-5 seconds.

2) example.com RADIUS server tries to authenticate victim@example.com from authentication backend (Active Directory, SQL, LDAP etc.)

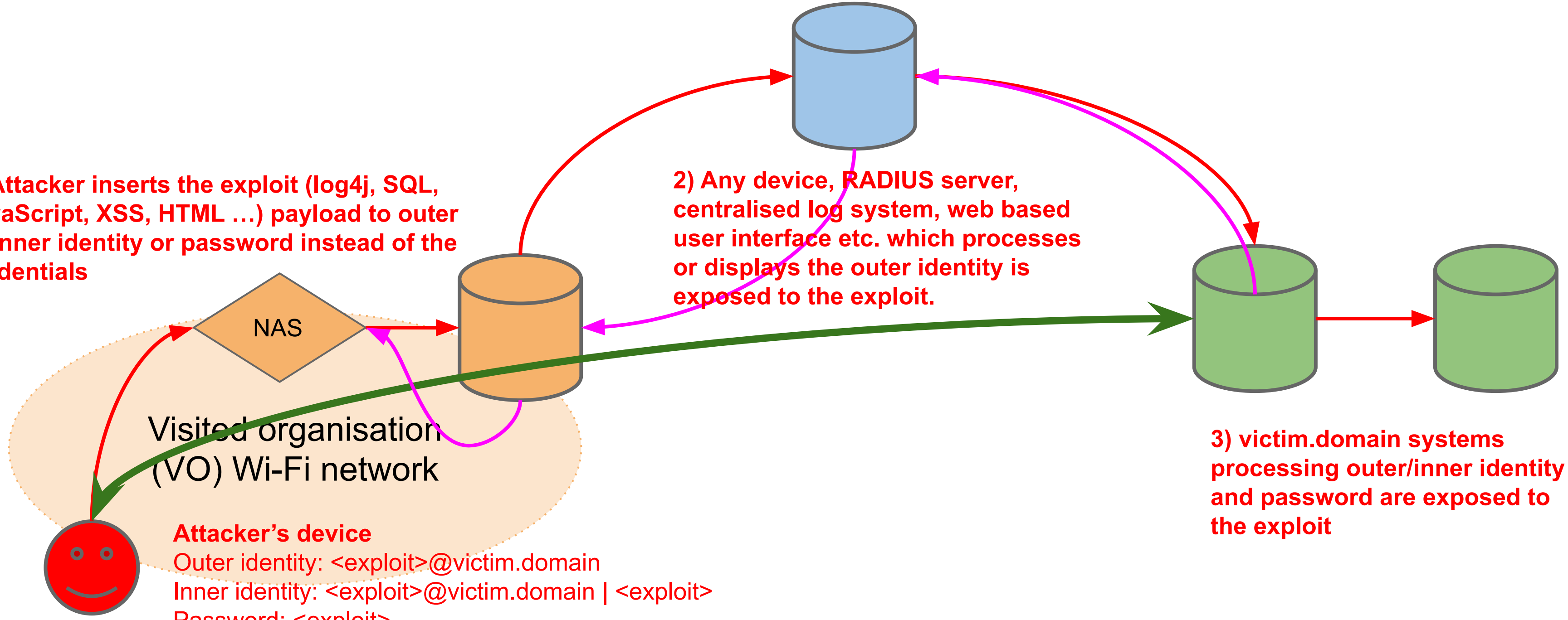
3) example.com RADIUS server authentication backend responds to all requests, but may also lock the user account for a while or completely (DoS)

Attacker’s device
Outer identity: anonymous@example.com
Inner identity: victim@example.com
Password: password guess

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



1) Attacker inserts the exploit (log4j, SQL, JavaScript, XSS, HTML …) payload to outer or inner identity or password instead of the credentials

NAS

Visited organisation (VO) Wi-Fi network

2) Any device, RADIUS server, centralised log system, web based user interface etc. which processes or displays the outer identity is exposed to the exploit.

3) victim.domain systems processing outer/inner identity and password are exposed to the exploit

Attacker's device
Outer identity: <exploit>@victim.domain
Inner identity: <exploit>@victim.domain | <exploit>
Password: <exploit>

Injection attack comments and mitigation

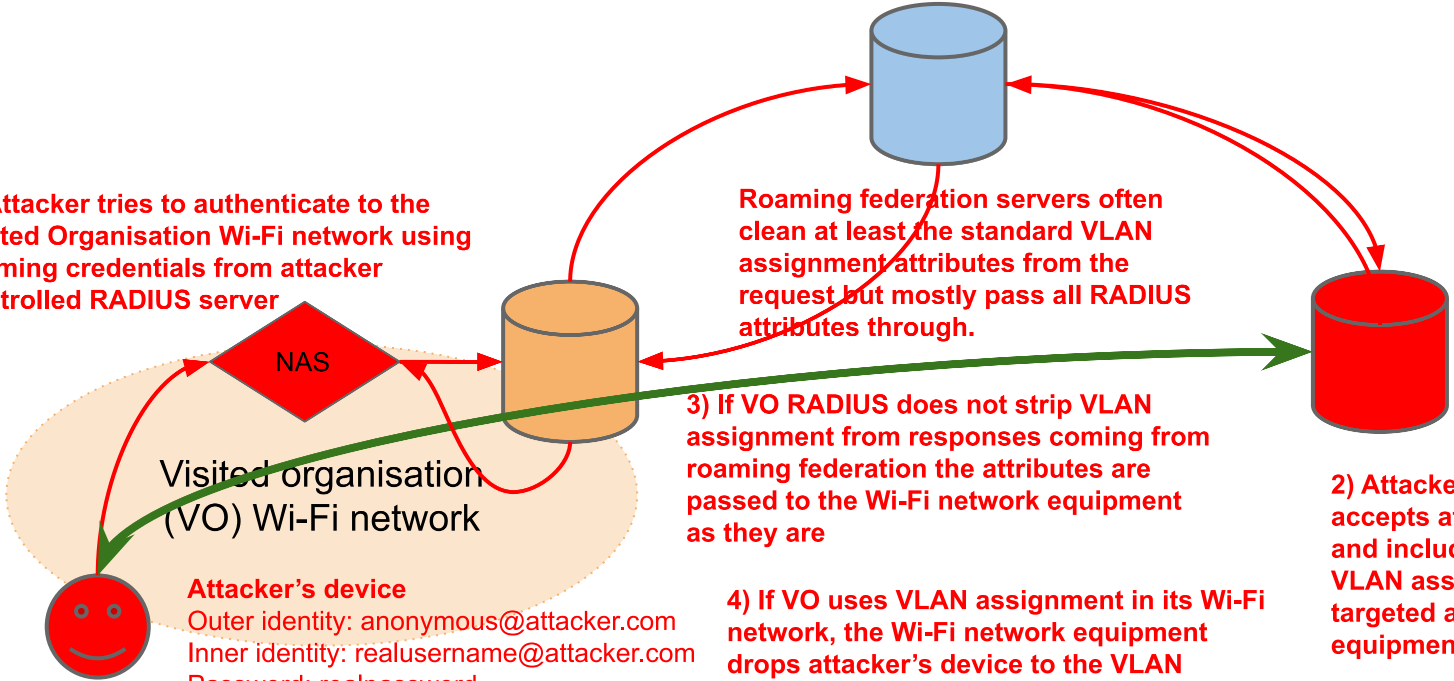
Comments

- 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 penetration attack



1) Attacker tries to authenticate to the Visited Organisation Wi-Fi network using roaming credentials from attacker controlled RADIUS server

Roaming federation servers often clean at least the standard VLAN assignment attributes from the request but mostly pass all RADIUS attributes through.

2) Attacker's RADIUS server accepts attacker authentication and includes in its response VLAN assignment attributes targeted at VO's Wi-Fi equipment.

3) If VO RADIUS does not strip VLAN assignment from responses coming from roaming federation the attributes are passed to the Wi-Fi network equipment as they are

4) If VO uses VLAN assignment in its Wi-Fi network, the Wi-Fi network equipment drops attacker's device to the VLAN defined by attacker's RADIUS server.

Attacker's device
Outer identity: anonymous@attacker.com
Inner identity: realusername@attacker.com
Password: realpassword

VLAN penetration attack mitigation

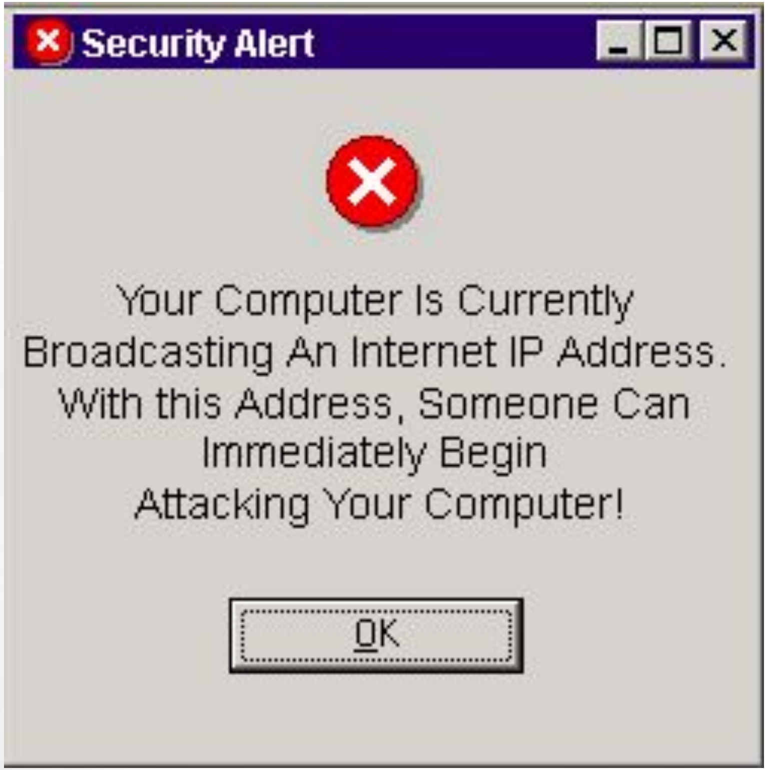
- Strip standard and vendor specific VLAN assignment RADIUS attributes in the own organisation RADIUS server
- Strip attributes in the other federation RADIUS servers
- Take care what organisations can join the roaming federation and in identifying them

TLS, PKI, etc.

- TLS versions have bugs, but to be interoperable, older TLS versions must still be accepted
- The only easy thing in TLS, PKI and certificates is to configure them incorrectly
- Detecting and diagnosing TLS attacks is hard
- Fortunately it is easier to benefit from other attacks than to focus on these ones
- Unfortunately that means that misconfigurations may not be noticed, because “everything works”

Wi-Fi Roaming Privacy

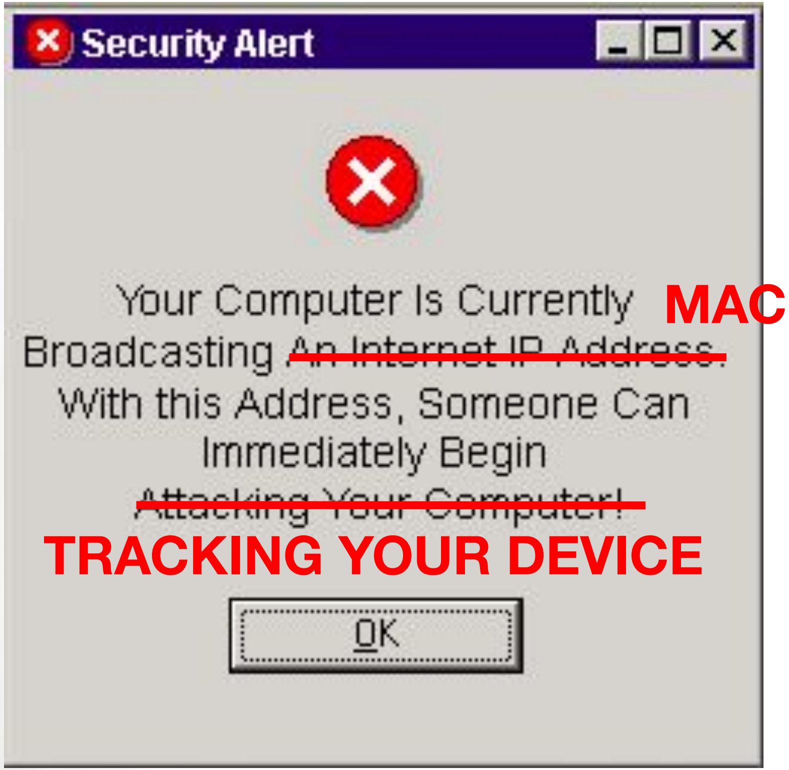
You may have seen this in the Internet …



Your Computer Is Currently Broadcasting An Internet IP Address. With this Address, Someone Can Immediately Begin Attacking Your Computer!

It’s funny, because it’s true…

(at least with these adjustments)



Your Computer Is Currently Broadcasting ~~An Internet IP Address.~~ MAC ADDRESS

With this Address, Someone Can Immediately Begin ~~Attacking Your Computer!~~

TRACKING YOUR DEVICE

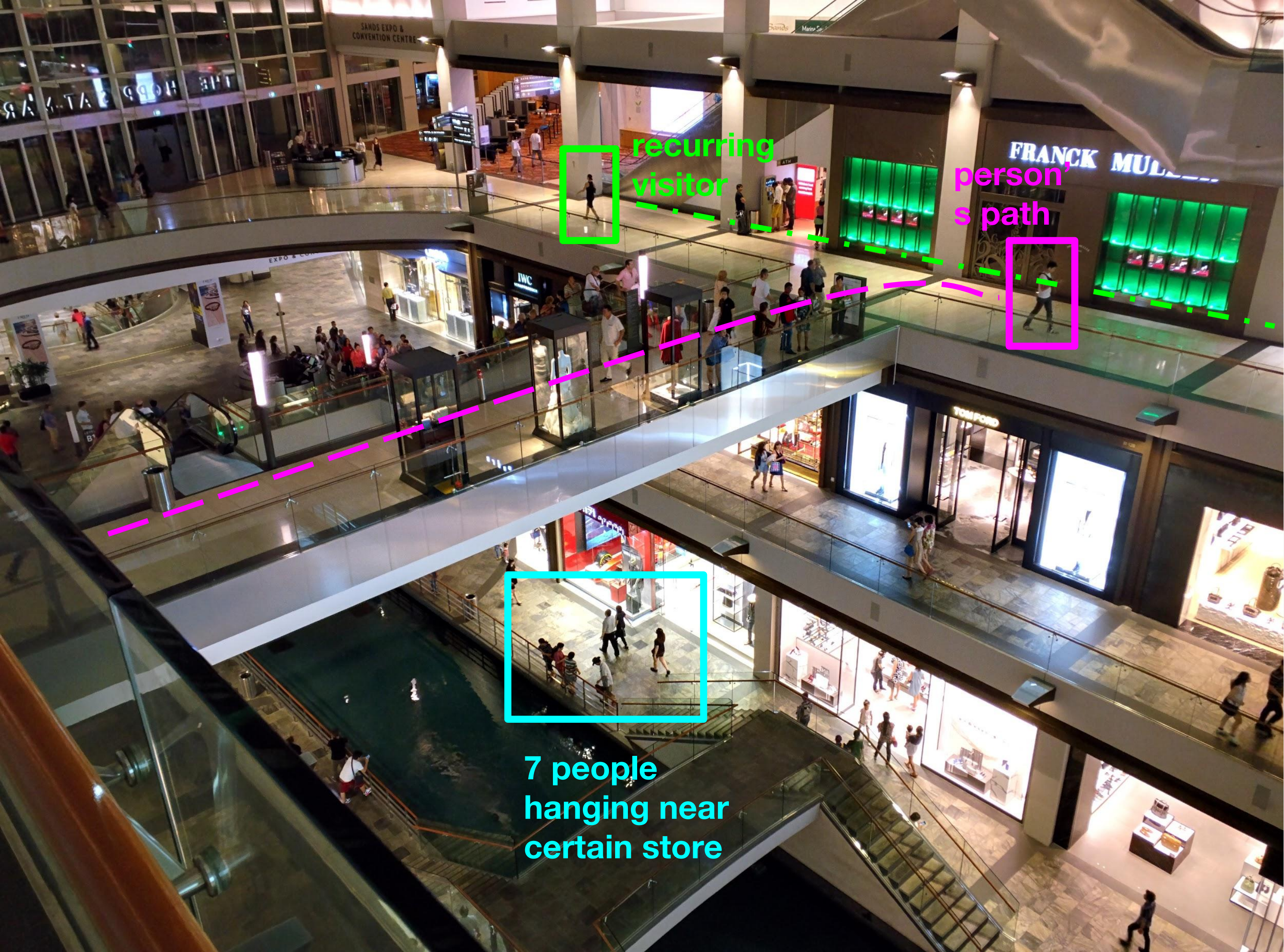
MAC addresses, we all got them...

- Most of **the network interfaces on your device** have a **unique address** called a **MAC address**

- **Wi-Fi** and **Bluetooth** interfaces may **“broadcast”** the address **even if the interface is not in active use**

MAC addresses are used ...

- to identify devices and users
- to control access to network
- to limit use of network resources
- to keep track of sessions
- to assign and track IP addresses
- to track devices => to track persons



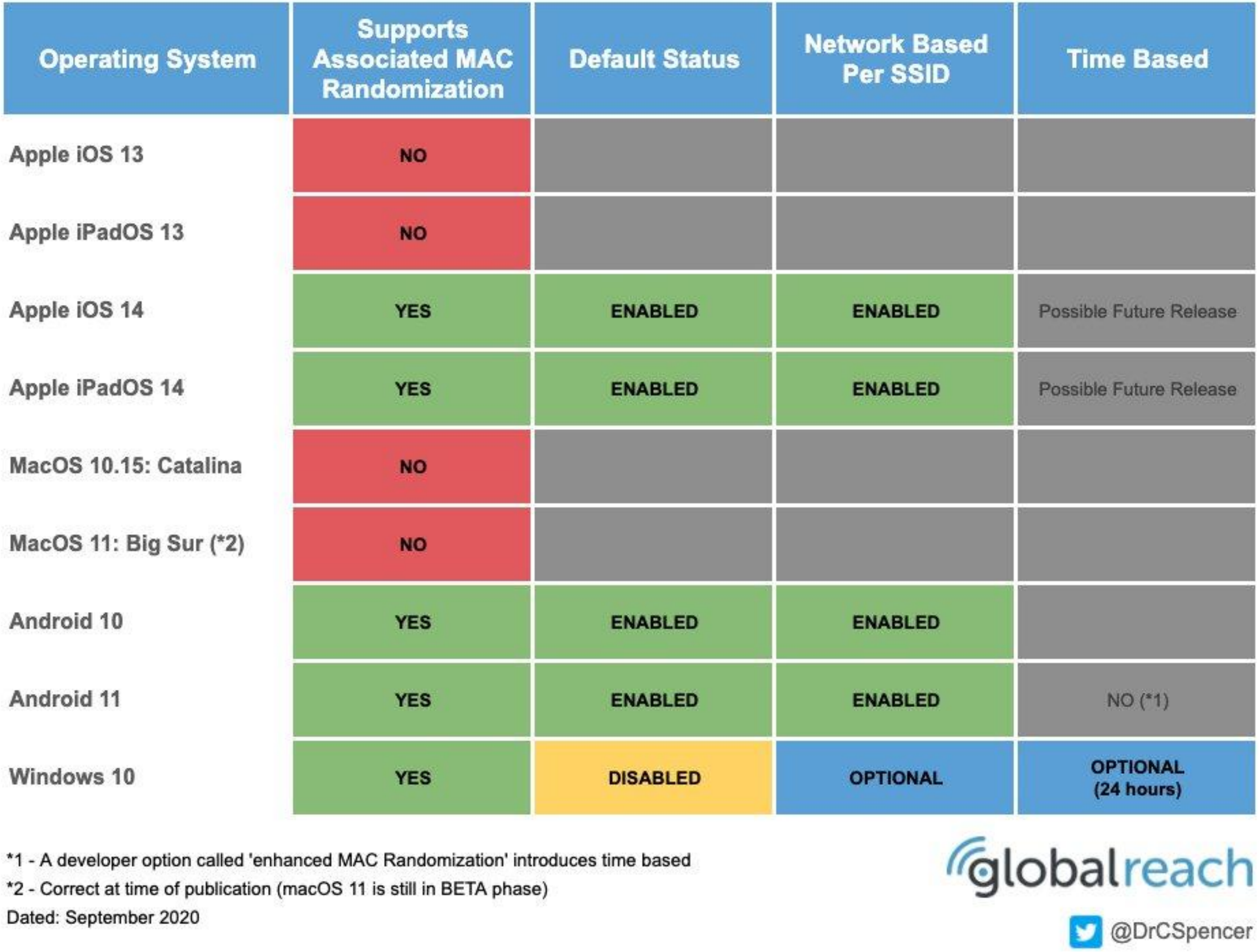
Wi-Fi devices send so called probe requests to find out what Wi-Fi networks are available and they may do this even if Wi-Fi is turned off.

Bluetooth devices respond to queries and may do own probing as well.

This makes it possible to track for example people and their movements in shopping malls. => nice tracking business.

MAC address randomisation

- first done only in the probe requests
- has been extended to network connections
- is currently per Wi-Fi network (profile)
- is expected in the future to be time-based as well
- is enabled by default in Android 10,11, iOS/iPadOS 14+



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

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

Randomised MAC address does not stop tracking

- In most devices randomised MAC address only changes when a network or profile is deleted and create again => recurring visitors can be identified at least within same network
- In authenticated and roaming networks MAC address does not really matter, User-Name and Chargeable-User-Identity can be used if these are not protected
- 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
- While WPA2/3 authentication protects RADIUS authentication with TLS, RADIUS accounting is sent in clear text

MAC addresses are not the only way to track you...

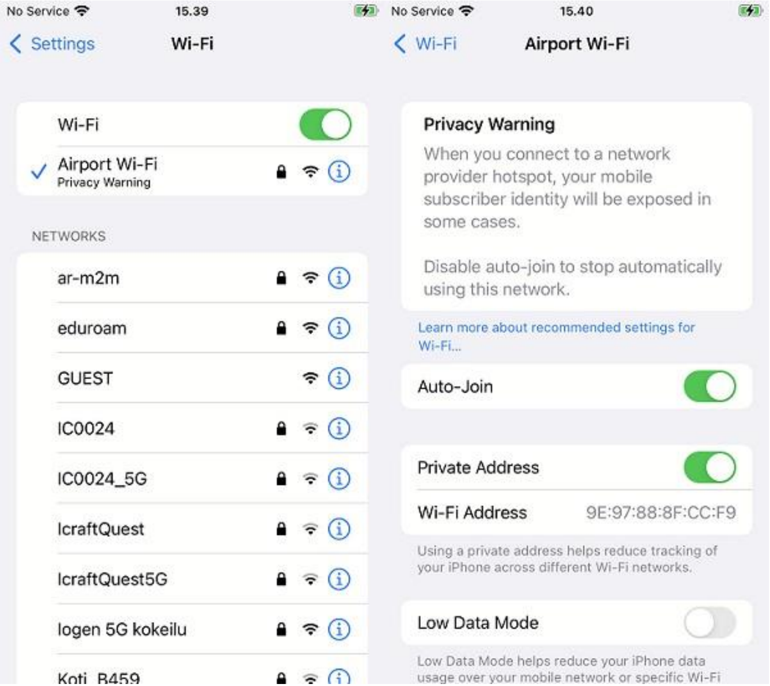
- Roaming network profiles make your device try to connect any network advertising suitable network name, roaming consortium organisation ID, realm etc.
- Your device may contain operator profiles not visible or manageable by you
- Even failed attempt to roam to the network may provide trackable information 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 to achieve seamless offloading to carrier and partner WiFi. International Mobile Subscriber Identifier (IMSI) derived from the SIM card is the unique identifier for each user.

On the first connection to a WiFi network, the mobile device communicates its permanent subscriber identity information (IMSI), which is then sent to the home operator for authentication. Without IMSI Privacy features, this identity is **sent in the clear.**

A potential 3rd party adversary installing a WiFi sniffer in the vicinity of such networks can harvest permanent identities and track users. This tracking can also be done by the venue or network owner when connecting to the WiFi network.



No Service 15.39

Settings Wi-Fi

Wi-Fi

✓ Airport Wi-Fi
Privacy Warning

NETWORKS

ar-m2m

eduroam

GUEST

IC0024

IC0024_5G

IcraftQuest

IcraftQuest5G

logen 5G kokeilu

Koti_B459

No Service 15.40

Wi-Fi Airport Wi-Fi

Privacy Warning

When you connect to a network provider hotspot, your mobile subscriber identity will be exposed in some cases.

Disable auto-join to stop automatically using this network.

Learn more about recommended settings for Wi-Fi...

Auto-Join

Private Address

Wi-Fi Address 9E:97:88:8F:CC:F9

Using a private address helps reduce tracking of your iPhone across different Wi-Fi networks.

Low Data Mode

Low Data Mode helps reduce your iPhone data usage over your mobile network or specific Wi-Fi

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

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.

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
d5b39070       Acct-Output-Gigawords = 0
```

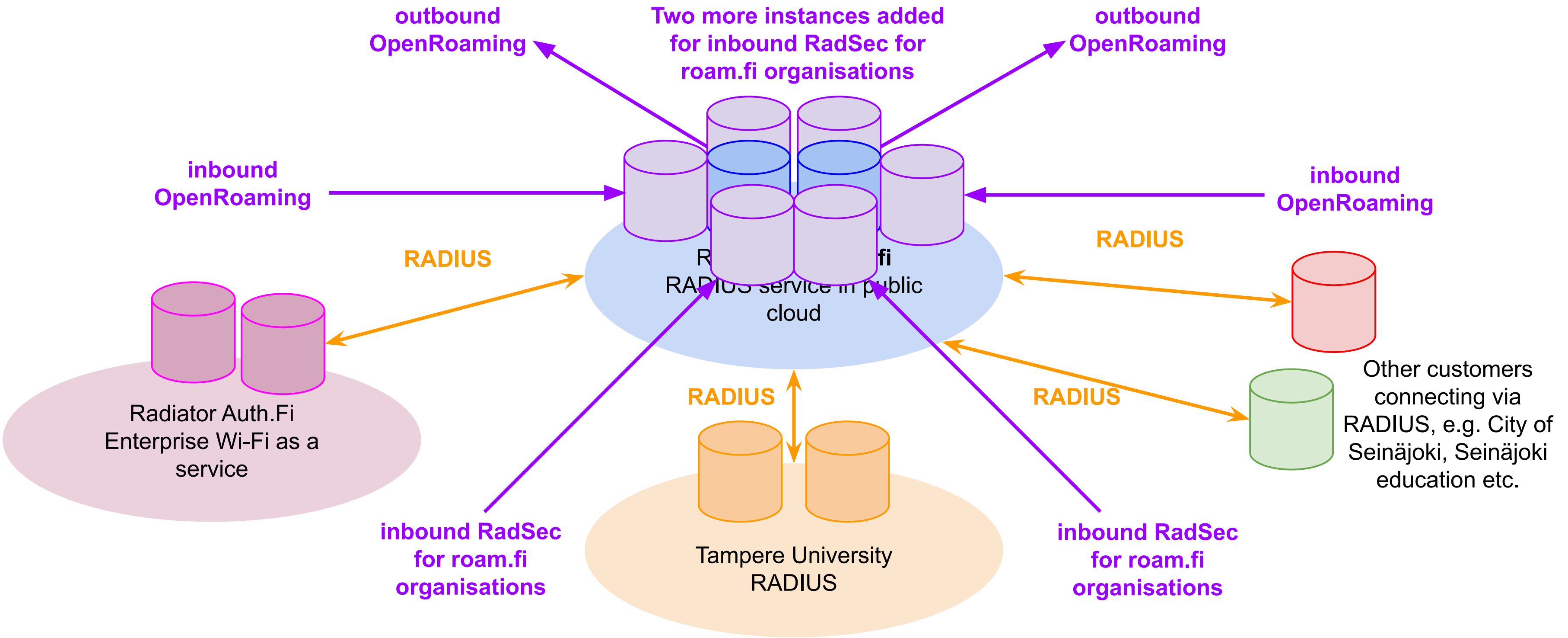
Note also one Location attribute. There are a lot more related attributes in the standardisation process and under development is also a technology called Wi-Fi sensing, which probably also brings new attributes to RADIUS requests.

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

How to protect privacy?

- Use MAC address randomisation
- 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 (OpenRoaming requirement)
- Use EAP-TLS with TLSv1.3 support for client certificate authentication
- Use IMSI Privacy Protection supporting clients, server software and operator

Adding RadSec to roam.fi roaming federation



outbound OpenRoaming

Two more instances added for inbound RadSec for roam.fi organisations

outbound OpenRoaming

inbound OpenRoaming

inbound OpenRoaming

RADIUS

RADIUS

R fi RADIUS service in public cloud

Radiator Auth.Fi Enterprise Wi-Fi as a service

RADIUS

RADIUS

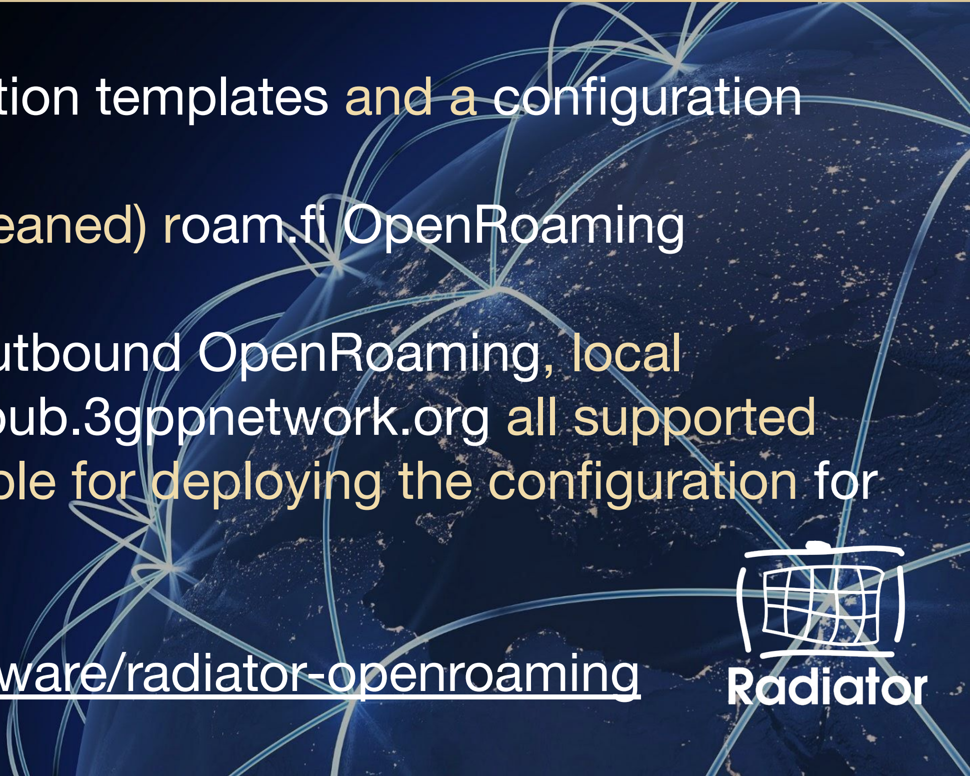
Other customers connecting via RADIUS, e.g. City of Seinäjoki, Seinäjoki education etc.

inbound RadSec for roam.fi organisations

Tampere University RADIUS

inbound RadSec for roam.fi organisations

Radiator OpenRoaming Configuration Repository



- Radiator architecture, configuration templates and a configuration guide for OpenRoaming
- Based on the presented (and cleaned) roam.fi OpenRoaming deployment and configuration
- Settlement-Free inbound and outbound OpenRoaming, local RadSec/RADIUS connectivity, pub.3gppnetwork.org all supported
- Workshops, consultation available for deploying the configuration for pilots or production
- Location (GitHub) any day now: https://github.com/radiator-software/radiator-openroaming

Radiator

Radiator

Next webinar coming up in June:

Radiator, OpenRoaming and IETF update

- Radiator 4.28 release highlights
- Radiator OpenRoaming enhancements
- Radiator OpenRoaming Configuration Guide update
- IETF standardisation and Radiator roadmap

Tue June 6 - 8AM UTC | 10AM CEST
Thu June 8 - 9AM PDT | 12NOON EDT

20TH ANNIVERSARY

Wireless Global Congress
Wireless Broadband Alliance

WGC AMERICAS

JUNE 19 – 22 2023

WI-FI INNOVATION:
FOR OPERATORS, ENTERPRISE, PLACES AND THINGS

Renaissance Las Vegas Hotel, USA

#WGCAMERICAS | #wifiinnovation | #wifirevolution | #lovewifi

Radiator

WGC Americas

We’re participating Wireless Global Congress
June 19-22 at Las Vegas, USA

book a meeting via info@radiatorsoftware.com

Radiator

Thank you!

Questions, comments?