

canarie



Get Serious about Wi-Fi Security:

Protect Users from Falling Victim to Credential Harvesting

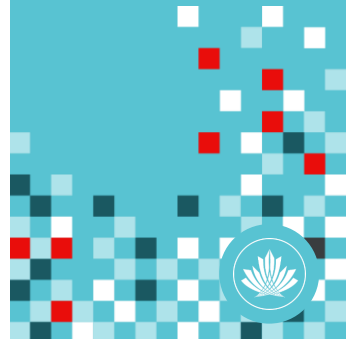
Ed Kingscote | DevOps Specialist

March 10, 2022

BCNET Connect Summit

eduroam Characteristics

- Globally distributed
- Bring-Your-Own-Device
- Secure
- Large-scale
- Widening reach

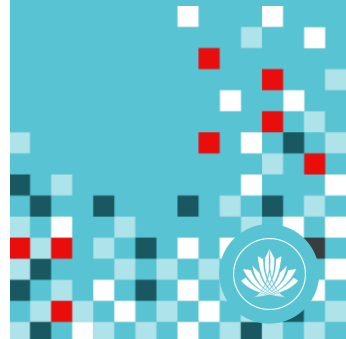




**Security is a practice,
not a thing.**

eduroam Security Features

- SSID
- Authentication
- Segregation
- Isolation
- Layers
- Guest Access
- Device Configuration
- PII Protection







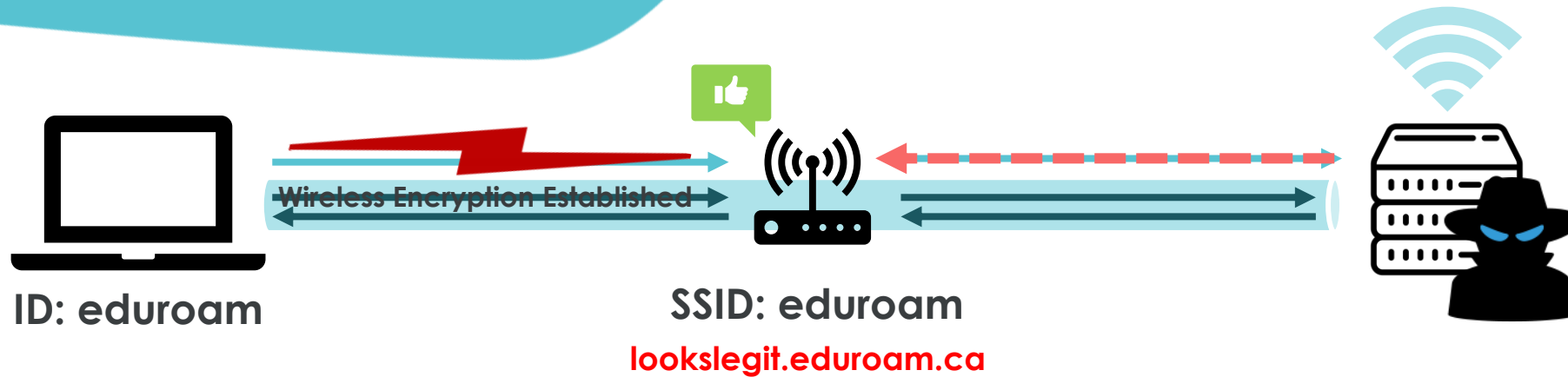
It's EAPHammer Time!

Demonstrating the Commoditized Harvesting of Wi-Fi Credentials

```
root@raspberrypi:/home/pi/eaphammer# ./eaphammer -i wlan0 --channel 4 --auth wpa-eap --essid eduroam --creds
```

I

What Happened?



1. Negotiate authentication model

EAP-PEAPv0-GTC, EAP-PEAPv0-MSCHAPv2

2. Certification validation (TLS Setup)

3. Establish secure tunnel (TLS)

Prevents eavesdropping

4. Perform authentication through tunnel

5. Authentication successful!

Establish encryption, connect to internet

6. Client acquires IP address (DHCP)





**It is the client's
responsibility to ensure that
they are communicating
with a trusted server.**

Mitigation – Next Steps

- Device Configuration
 - Setup eduroam CAT Profile
 - User device enrolment
- Enforcement
 - For an institution
 - For roaming



Mitigation: Device Configuration

Set Up eduroam CAT Profile

General Profile properties

Profile Name and RADIUS realm

Profile Description (default/other languages) **profile for testing anonymous outer identity**

Profile Display Name (default/other languages) **anonymous validator.eduroam.ca profile**

Production-Ready **on**

Add new option

Realm:

Realm Options

Outer Identity Handling

Enable Anonymous Outer Identity:

Use special Outer Identity for realm checks:

Inner Identity (Username) Handling

Enforce realm suffix in username

Enforce exact realm in username

Installer Download Location

Redirect end users to own web page:

Supported EAP types

Supported EAP types for this profile

1. PEAP-MSCHAPv2

Unsupported EAP types

FAST-GTC

EAP-pwd

TLS

TTLS-GTC

TTLS-MSCHAPv2

TTLS-PAP

Managed IdP

Use "drag & drop" to mark an EAP method and move it to the supported (green) area. Prioritisation is done automatically, depending on where you "drop" the method.

EAP Details for this profile

CA Certificate File

CA Certificate File

Name (CN) of Authentication Server **dcx.caftest.canarie.ca**

Add new option

<https://cat.eduroam.org/>



Mitigation: Device Configuration

User Device Enrolment

- Android 11+/Apple/Microsoft
 - geteduroam.app / App Stores
- Linux, Android 4.3-10, ChromeOS
 - <https://cat.eduroam.org>



Image © User:Rdevany / Wikimedia Commons / CC-BY-SA-3.0



Mitigation: Enforcement Institution

- Audit
- Communicate
- Enroll
- Enforce

Connection Request Policies

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

Policy Name	Status	Processing Order	Source
caftest2.eduroam.ca realm - Permit Correct OuterID	Enabled	1	Unspecified
caftest2.eduroam.ca realm - Force Reject of No AnonOuterID	Enabled	2	Unspecified
validator.eduroam.ca realm	Enabled	3	Unspecified
caftest.canarie.ca realm	Enabled	4	Unspecified
caftest.eduroam.ca realm	Enabled	5	Unspecified
surf.testeduroam.ca realm	Disabled	6	Unspecified
eduroam.ca realm	Disabled	7	Unspecified
EDUROAM visitors	Enabled	8	Unspecified
Use Windows authentication for all users	Disabled	9	Unspecified

caftest2.eduroam.ca realm - Permit Correct OuterID

Conditions - If the following conditions are met:

Condition	Value
User Name	anonymous911911@caftest2\eduroam\ca\$

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer
Extensible Authentication Protocol Configuration	Configured
Extensible Authentication Protocol Method	Microsoft: Protected EAP (PEAP)
Authentication Method	EAP
Override Authentication	Enabled

Connection Request Policies

Connection request policies allow you to designate whether connection requests are processed locally or forwarded to remote RADIUS servers.

Policy Name	Status	Processing Order	Source
caftest2.eduroam.ca realm - Permit Correct OuterID	Enabled	1	Unspecified
caftest2.eduroam.ca realm - Force Reject of No AnonOuterID	Enabled	2	Unspecified
validator.eduroam.ca realm	Enabled	3	Unspecified
caftest.canarie.ca realm	Enabled	4	Unspecified
caftest.eduroam.ca realm	Enabled	5	Unspecified
surf.testeduroam.ca realm	Disabled	6	Unspecified
eduroam.ca realm	Disabled	7	Unspecified
EDUROAM visitors	Enabled	8	Unspecified
Use Windows authentication for all users	Disabled	9	Unspecified

caftest2.eduroam.ca realm - Force Reject of No AnonOuterID

Conditions - If the following conditions are met:

Condition	Value
User Name	.caftest2\eduroam\ca\$

Settings - Then the following settings are applied:

Setting	Value
Authentication Provider	Local Computer
Manipulation Target Attribute	User Name
Manipulation Attribute Rules	Replace "@caftest2.eduroam.ca" with "@missingouterid"
Override Authentication	Disabled



Mitigation: Enforcement

Roaming via the Canadian Access Federation (CAF)

- Enforce Anonymous Outer ID
- Scope
- Impact

SSID: eduroam

CERT: eduroam.home_institution.ca

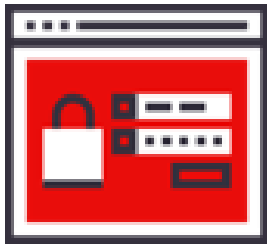




Phishing is not tolerated.

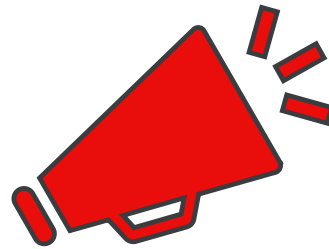
**eduroam Wi-Fi credential
harvesting shouldn't be either.**

Conclusion



Configure

CAT Profile



Communicate

Educate users on geteduroam
app (Apple, Android, Microsoft)

or

cat.eduroam.org (Linux etc.)

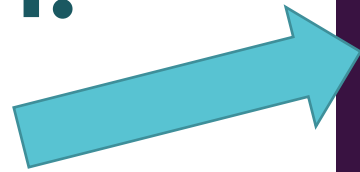


**Start
Enforcement**

Deny access



Let's continue the conversation!



CANARIE CAF-FCA ▼ 

CANARIE CAF-FCA
canarie-caf-fca.slack.com

Channels ⋮ +

- # announcements
- # eduroam
- # eduroam-cat-profile
- # eduroam-tech-talk
- # eva
- # eva-tech-talk
- # events
- # fim
- # fim-shibboleth-v4-upgrade
- # fim-tech-talk
- # help
- # welcome







canarie



canarie.ca | [@canarie_inc](https://twitter.com/canarie_inc)



CAF Support: tickets@canarie.ca
ed.kingscote@canarie.ca