OpenRoaming/MADINAS
@IETF118Hackathon

Mark Grayson, Bruno Tomas
Background

- OpenRoaming Federation described in draft-tomas-openroaming
- OpenRoaming listed in Existing-Solutions section of draft-ietf-madinas-use-cases
  … offering the possibility for the user or the device to keep their identity obfuscated from the local network operator …
- IETF117 presentation of some experiences with OpenRoaming
  Presented logs from limited number of authentication exchanges, indicating privacy leakage across RADIUS interface between Identity Provider and Access Provider
OpenRoaming @ IETF118 Hackathon

• Hackathon aims:
  Analyse the possible leakage of privacy information by a variety of OpenRoaming Identity Providers (IDPs) for a variety of different OpenRoaming Access Network Provider (ANP) use-cases

• Capture authentications exchanges between different access network implementations and wide range of production OpenRoaming Identity Providers
Hackathon OpenRoaming Access Networks

- Cisco Catalyst
- Cisco HS Connector
- Radiator AP
- Radiator Proxy
- Cisco Meraki
- RadSec Proxy
- UC3M MikroTik
- RadSec Proxy

IETF MikroTik
OpenRoaming UC3M
Authentication logs captured with the following OpenRoaming IDP Realms

1. apple.openroaming.net
2. eu-google.openroaming.net
3. wlan.mnc280.mcc310.3gppnetwork.org
4. wlan.mnc150.mcc310.3gppnetwork.org
5. clus.openroaming.net
6. odysys.net
7. wlan.mnc410.mcc310.3gppnetwork.org
8. wba.3af521.net
9. profile.guglielmo.biz
10. openroaming.securewifi.io
11. openro.am
12. openroaming.goog
13. tokyo.wi2.cityroam.jp
14. ironwifi.net
15. radiatorsoftware.com
User-Name/NAI Observations

- All PLMN-IDs operate using EAK-AKA with pseudonyms, identified using leading character “2”
  E.g., User-Name: 2NP0z9iN0l+pZ7gcUkO55mn@wlan.mnc280.mcc310.3gppnetwork.org
- All other non EAP-AKA methods use anonymous@realm
- The following realms re-write User-Name in Access-Accept:
  eu-google.openroaming.net, apple.openroaming.net, clus.openroaming.net, e.g.,
  - Access-Request: User-Name: anonymous@apple.openroaming.net,
  - Access-Accept: User-Name: 4ce6d90b-7a5a-40e0-84a7-888faba2c0d4@apple.openroaming.net
Class Observations

- odyssey.net is only realm that does not return CUI and only non PLMN realm to return Class
  

- All three PLMNs return three Class attributes:
  1. Static Class looks to be used by a Roaming Gateway
     
     Class: fD/rgwx/aai:16777264
  2. User variable Class
     
     Class: BIC:931082D5E1AD404995CF2FC98AD5545919057EC8DD94C495
  3. Class which looks to embed diameter routing and user IMSI
     
     Class: Diameter/dal-0019.rmr.corp.wayport.net;1699084922;723241;0310410141640351@wlan.mnc410.mcc310.3gppnetwork.org;dal-0019.rmr.corp.wayport.net
CUI Observations

- Uncontrolled Hackathon environment was not conducive to logging mobility events between different OpenRoaming access networks.
- One IDPs (eu-google.openroaming.net) has user explicit opt in with IDP to share email identity with ANP – in which case email address is returned in CUI.
- clus.openroaming.net returns a fixed value testuser@clus.openroaming.net.
- wba.3af521.net and openroaming.securewifi.io realms did not return any CUI or Class.
Examples of Encoded CUI

• wlan.mnc280.mcc310.3gppnetwork.org
  CUI: 6c21d5a2e64f72d31046ea8cbe5b7a5bc66c808f
• apple.openroaming.net
  CUI: 020cc1c0-a441-4e01-9f91-e3b65243f932@openroamingapple
• openroaming.goog
  CUI: u3gBZSZiYqvvRI37ORX_1HxwjFZg-dB8hsbvz8Oeaiv_uzUwo-2a-TKE_-BGKFn QCIV6YNCnxnwp0dMVf3NAtd_9
• tokyo.wi2.cityroam.jp
  CUI: R02NYVS835
Key Take-Aways - 1

- Confirmed Attributes in Access-Accept can be used to leak privacy information.
- Since presentation of OpenRoaming experiences at IETF117, draft-ietf-radext-deprecating-radius has added a section on Minimizing Personal Identifiable Information.

Currently focuses on CUI with a recommended CUI construction:

\[ \text{CUI} = \text{HASH(visited network data + user identifier + key)} \]

- Examples of User-Name rewrite and Class observed that are unlikely to correspond to hashed user identifier, e.g.:
  
  User-Name: 4ce6d90b-7a5a-40e0-84a7-888faba2c0d4@apple.openroaming.net
  
  Class: ….;0310410141640351@wlan.mnc410.mcc310.3gppnetwork.org;…
Key Take-Aways - 2

- Examples of CUI and Class observed that may correspond to hashed user identifier, e.g.:

  Class:
  GRT????*?S??k^HO?+?_??7??ej??V??E?+B>i?Y:?=?i????k>??P@[?
  ?\r??

  Class:
  BIC:931082D5E1AD404995CF2FC98AD5545919057EC8DD94C495
  CUI: 6c21d5a2e64f72d31046ea8cbe5b7a5bc66c808f
  CUI: u3gBZSZiYqvvl37ORX_1HxwjFZg-dB8hsbvz8Oeaiv_uzUwo-
  2a-TKE_-BGKFnQClV6YNClxnwp0dMVf3NAtd_9
  CUI: R02NYVS835
Key Actions/Considerations

• Does the radext I-D need to be enhanced with sections on User-Name rewrite and Class?
• Should OpenRoaming federation specify use of hashed identifiers in Access-Accept, unless the user has explicitly agreed to terms that permit sharing of permanent identifiers?
Thanks to Hackathon Participants

Bart Brinckman, Bruno Tomas, Carlos Bernardos, Fabian Mauchle, Juan-Carlos Zuinga, Karri Huhtanen, Heikki Vatiainen, Mark Grayson, Subir Das