Date	23rd February 2024	**Meeting Time**	N/A
WG / Project	WBA OpenRoaming Work Group		
To	IETF RADEXT WG IETD MADINAS WG		
Project chaired by	Mark Grayson (Cisco) Betty Cockrell (Single Digits) Necati Canpolat (Intel)		
Topic	Privacy leakage across the OpenRoaming federation		
Action ID Prefix	N/A		

Dear Members of IETF MADINAS and RADEXT Working Groups,

The Wireless Broadband Alliance (WBA) would like to share recent updates concerning its WRIX and OpenRoaming Specifications that are pertinent to the two working groups.

Background

WBA has recently liaised with both MADINAS and RADEXT Working Groups, first introducing the OpenRoaming federation (https://datatracker.ietf.org/liaison/1848/) as well as more recently around the topic of privacy leakage across the federation (https://datatracker.ietf.org/liaison/1862/).

Subsequently at IETF118, WBA members participated in the OpenRoaming hackathon aimed at analyzing the possible leakage of privacy information by a variety of OpenRoaming identity providers for a variety of different OpenRoaming access network provider use-cases. Results presented confirmed that certain OpenRoaming identity providers were configuring attributes in the RADIUS Access-Accept message that could weaken the privacy of end-users (https://datatracker.ietf.org/meeting/118/materials/slides-118-madinas-hackathon-openroaming-update-00).

Recent Updates

WBA would like to share with MADINAS and RADEXT working groups that it has now updated its WRIX and OpenRoaming specifications to include normative text regarding end-user privacy, aimed at preventing the unintentional weakening of end-user privacy by the use of correlation identifiers in RADIUS Access-Accept messages.

WBA now recommends that the default identity provider policy should ensure that any correlation identifiers in the RADIUS Access-Accept message, such as Class attribute (#25) and/or Chargeable-User-Identity attribute (#89), are unique for each combination of end-user and access network provider and that the keys and/or initialization vectors used in creating such correlation identifiers should be refreshed at least every 48 hours, but not more frequently than every two hours.

This two hour limit is designed to permit the access network provider to perform autonomous troubleshooting of connectivity issues from authentic users/devices that are repeatedly re-initiating connectivity to the access provider's network and/or permit the access provider to identify a new session originated by an authentic user/device that has previously violated the OpenRoaming end-user terms and conditions.

In contrast to this default policy, WBA WRIX specifications describe scenarios where the 48 hour limit is required to be extended, for example when the identity provider supports settled service and requires the correlation identifier to be stable over an entire billing period.

WBA has worked with the authors of OpenRoaming I-D to update the draft to reflect these recent changes (https://www.ietf.org/archive/id/draft-tomas-openroaming-02.html).

WBA plans to communicate these changes to all OpenRoaming identity providers to ensure they are aware of the updated recommendations.

Request

WBA would welcome the opportunity to present the OpenRoaming I-D to the RADEXT WG at IETF 119.

For more information, please contact the WBA PMO (pmo@wballiance.com)

Upcoming WBA Working Sessions:

- Dallas 10-13th June
- Paris 7-10th October