DULT WG Accessory Protocol (Document #3)

DULT WG meeting #4
IETF #122
March 2025

Agenda

- Discuss two GitHub issues
- Next steps

Issues

1. Printing Non-SN Unique Identifiers
2. Remote disablement

Printing non-SN unique identifiers

- Issue: https://github.com/ietf-wg-dult/accessory-protocol/issues/2
- From 12/21/2023: @cstapl: “Strong concerns that we’re making an allowance for vendors to opt out of printing the unique identifier in an easily accessible location on the physical device. It’s my understanding that those identifiers are a critical part of the physical evidence in law enforcement response to unwanted tracking related calls from victims, and in the prosecution of such cases. Recommend we discuss this issue with victim advocacy groups, and consider requiring all identifiers to be printed on the physical device.”
- Issue at hand is that Accessory Protocol allows for privacy-preserving identifier, which rotates over time
- How do people feel about this?

3.15. Identification

The accessory **MUST** include a way to uniquely identify it - either via a serial number or other privacy-preserving solution. Guidelines for serial numbers only apply if the accessory supports identification via a serial number.

3.15.1. Serial number identification

If a serial number is available, it **SHALL** be printed and be easily accessible on the accessory. The serial number **MUST** be unique for each product ID.

Additional information and point of view:

- Benefits of printing a serial number may vary depending on the identifier type the network operates on.
- If there is no serial number, or the network does not use this particular number for identification, it limits the benefit of the printed number.
- In this case, a printed serial number cannot be used to identify the owner, but it might be used only as a visual evidence.

Remote Disablement

- [New] issue: https://github.com/ietf-wg-dult/accessory-protocol/issues/14
- There might be situations where the tracker is very well hidden and its speaker is removed.
- Despite receiving multiple alerts on their phone, the victim might not locate the tag and disable it.
- Question/discussion: Should the accessory protocol allow remote disablement of trackers and include recommendations/requirements about it?

3.14. Disablement

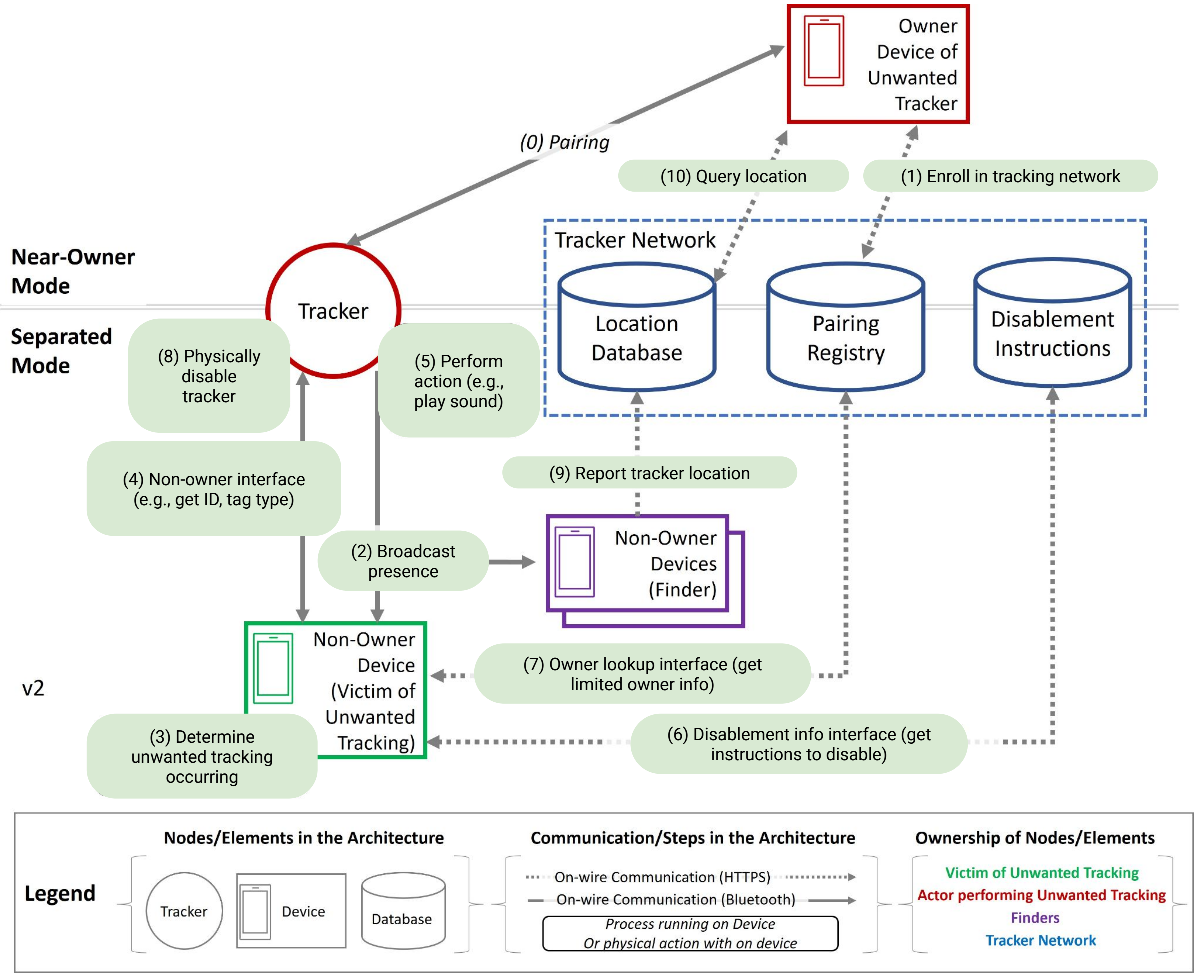
The accessory SHALL have a way to be disabled such that its future locations cannot be seen by its owner. Disablement SHALL be done via some physical action (e.g., button press, gesture, removal of battery, etc.).

Next steps

- Some work to close out issues discussed in IETF #121
- Any additional issues we want to discuss today?
- Would love people to file more issues on GitHub

Questions?

Back-up



State	In scope?
(1) Enroll in Tracking Network	**Yes:** *Design mechanisms to ensure that devices that do not correctly implement or adhere to the DULT protocol can be detected and excluded...*
(2) Broadcast Presence	**Yes:** *Allow a tracking accessory to identify & advertise its presence....*
(3) Determine unwanted tracking occurred	**Yes:** *Reference algorithm in scope of charter...*
(4) Non-Owner Interface	**Yes:** *Allow a nearby device to trigger behavior...*
(5) Perform Action	
(6) Disablement Info Interface	**Yes:** *Allow nearby devices to fetch additional information about a tracker accessory...*
(7) Owner Lookup Interface	
(8) Disable Tracker	**Yes:** *Includes physical security considerations, such as user impact when device has been physically modified to diminish findability...*
(9) Report location	**Yes:** *Design mechanisms to ensure that devices that do not correctly implement or adhere to the DULT protocol can be detected and excluded...*
(10) Query location	