Detecting Unwanted Location Trackers

BoF #2 Presentation
November 6, 2023

Summary of updates to draft charter

Summary of changes made

1. Added entire BT advertisement as in scope (as is NFC payload)
2. Added security and privacy requirements and considerations of the finding network are in scope
3. Added detecting non-conformant trackers as in scope
4. Added physical security for trackers is in scope
5. Added considerations for people w/o devices as in scope
6. Fixed minor typos + added clarifications as-needed
7. Apple submitted updated IPR disclosures on 10/12/2023

All charter additions highlighted in ***bold italic font*** in following slides

DULT Draft Charter

Background

Location-tracking accessories provide numerous benefits to users (e.g., such as being able to find where they left their keys), but can also have security and privacy implications if used for malicious purposes. These accessories can be misused to track another person’s location without their knowledge.

To address this threat, accessory manufacturers have developed independent solutions for protecting users from unwanted tracking. However, this requires users to know about the threat of unwanted tracking, download multiple apps, and constantly be checking for the threat of unwanted tracking. In order to build a scalable solution for detecting unwanted tracking, trackers require a consistent protocol and set of behaviors that will enable protection from unwanted tracking using any tracker.

DULT Draft Charter

Goals

The goal of the DULT WG is to standardize an ***application*** protocol for information exchange between location-tracking accessories and nearby devices, along with actions that these accessories and devices should take once unwanted tracking is detected. ***This protocol is intended to protect people against being unknowingly tracked. The intent of this WG is to make it easier for arbitrary devices to detect unwanted tracking by these accessories.*** The protocols and interactions between devices may be limited to certain states or modes, such as the accessory being separated from a paired/owner device.

The working group will define privacy and security properties of its solution, including privacy and security protections for tag owners when tags are used appropriately, and evaluate the tradeoffs.

The WG protocol design will be guided by an intent to:

- Minimize hardware changes needed in tracking accessories to implement this protocol; and
- Not preclude adoption by manufacturers of larger devices whose primary purpose is not location tracking, but have location tracking capabilities (e.g., headphones, bicycle, smartphone)

DULT Draft Charter

Program of Work

The WG is expected to:

1. Standardize a protocol ***("DULT protocol")*** between tracking accessories and nearby devices, which may:
    - Allow a tracking accessory to identify & advertise its presence when in a detectable mode, ***using standard formats defined for the underlying transports (e.g., BT, NFC, etc.)***
    - Allow a nearby device to trigger behavior on an unwanted tracking accessory to aid in determining its physical location
    - Allow nearby devices to fetch additional information about a tracker accessory***, including such things as tracker image asset(s) and physical disablement instructions***
    - ***Add privacy and security requirements or considerations for all messages used for advertisement, interactions with crowdsourcing networks, and owners of accessories***
2. Specify practices that accessory manufacturers can implement to deter malicious use of tracking accessories and support the implementation of the WG-specified protocol.
    - ***Include physical security considerations, such as user impact when device has been physically modified to diminish detectability and/or findability***
    - ***Include considerations for protecting people that don't have a device capable of running a platform-based unwanted tracking detection system***

DULT Draft Charter

3. Specify guidance for non-owner device platforms necessary to support implementation of the DULT protocol.

4. Carry out a threat analysis and security analysis before publishing protocol

5. Design mechanisms to ensure that devices that do not correctly implement or adhere to the DULT protocol can be detected and excluded from being trackable via crowdsourced location networks.

- ***This includes considerations for addressing legacy trackers that cannot update to the DULT protocol.***

The WG will not standardize an end-to-end platform-based unwanted tracking detection system or define requirements for interactions between accessory manufacturers and law enforcement. ***Phones, tablets, watches, and laptops are not considered accessories and are out of scope for this working group.***

Since most of the existing tracking accessories use Bluetooth, the DULT WG will coordinate as needed with the IETF 6lo WG and Bluetooth SIG.

DULT Draft Charter

Milestones

- Submit an informational document about the state of tracker accessory platforms and how they work for publication
- Submit a standards document defining the protocol to detect and interact with unwanted tracker accessories for publication