DULT Updated Technical Threat Model

Maggie Delano, Swarthmore College
Jessie Lowell, Safety Net Project, NNEDV

Motivation

- In order for the DULT protocol to be successful, the WG will need an understanding of an unwanted tracking threat model

- Document 4 has recently been adopted by the WG and includes:
  - A taxonomy of unwanted tracking
  - What we think should be in/out of scope w.r.t. attackers and victims
  - Design considerations for protocols

- Further work on the technical specifications and likely threats are needed to evaluate the proposed DULT protocols

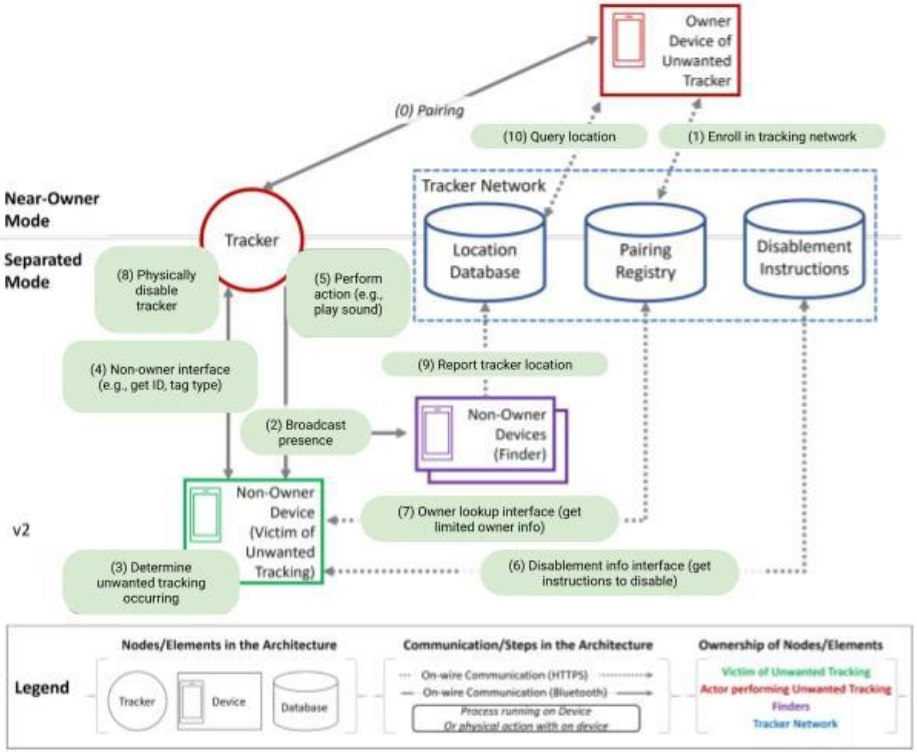
Definitions (review)

active scanning: a search for location trackers manually initiated by a user

passive scanning: a search for location trackers running in the background, often accompanied by notifications for the user

tracking tag: a small, concealable device that broadcasts location data to other devices

DULT Architecture (review)



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	

Threat Model Taxonomy (review)

- Attackers and victims can have different levels of expertise, access to resources/technological safeguards, and proximity
- Tracking tag usage can be attacker only, victim only, or both attacker and victim
- Example scenarios can be found in Document 4 or the presentation from IETF 119

What (we propose) is in scope for DULT WG (review)

- Technologies
  - Any easily-concealable accessory that is able to broadcast its location to other consumer devices
- Attacker Profiles
  - Attacks using platform native tracking applications
  - Attacks that include physical modifications of a tracking tag
  - Non-nation-state level alterations to firmware or deployment of custom devices that leverage crowdsourced tracking network
- Victim Profiles
  - All in scope regardless of expertise, resources, or access to technological safeguards

What (we propose) is out of scope for DULT WG (review)

- Technologies
  - App-based technologies such as parental monitoring apps
  - Tracking tags or other IoT devices or that are not easily concealable
  - Connected cars
  - User accounts for cloud services or social media
- Attacker Profiles
  - Attackers with nation-state level expertise and resources (e.g. cracking encryption)
  - Jailbreaking of a victim’s device
- Victim Profiles
  - N/A

Design Considerations (review)

- Include a variety of approaches to address different scenarios, including active and passive scanning and notifications or sounds
- Account for scenarios in which the attacker has high expertise, proximity, and/or access to resources within scope
- Account for scenarios in which the victim has low expertise, access to resources, and/or access to technological safeguards within scope
- Avoid privacy compromises for the tag owner when protecting against unwanted location tracking using tracking tags
- Variety of notification modalities (e.g. non-audio option for Deaf victims)

Proposed Technical Specifications

- Attacks on DULT Architecture
- Unwanted Location Tracking Scenarios
- Design Constraints
- Design Requirements

Proposed Attacks In Scope

High priority threats include:

- Multiple tags following single victim
- Non-compliant tag (e.g. speaker disabled)
- Remote advertisement monitoring
- Spoofed tag

Proposed Tracking Scenarios In Scope

High priority scenarios to address include:

- Tag placement
  - Tag placed on victim's person or immediate belongings
  - Tag(s) in proximity to victim but not on their person (e.g. child's backpack, car)
  - Tags nearby but not used for unwanted location tracking (e.g. false positives by family or on transit)
- Anticipation of unwanted location tracking
  - Support for potential victims who are actively looking for potential tags (i.e. active scanning)
  - Support for potential victims who are not actively looking for potential tags (i.e. passive notifications)

Proposed Constraints

Constraints include (feedback from industry esp. welcome):

- BLE protocol constraints (e.g. packet size, public advertisements)
- Power constraints (protocol cannot have large impact on battery life)
- Device constraints (protocol must be supported by existing hardware/software, should not require new designs)

Proposed Requirements

- Users should be able to actively scan their location for devices that might be tracking them
  - This scan should take less than Y minutes (5-10?)
  - These scans should not trigger on devices that are nearby their owners
- Protocol should be able to detect an unwanted location tracker passively within X minutes (15? 60? customizable?)
  - Acceptable false positive rate?
  - Acceptable false negative rate?
- Tags that are separated from their owners should notify nearby users (how often?)
- Users should be able to customize their settings such as:
  - Notification frequency
  - Notification type (sound, vibration, alert)
  - Unwanted tracking algorithm sensitivity (e.g. low/medium/high)
- Platform should assist user in locating trackers
  - Users should be able to disable tracker (remotely?)

Open Questions

- What parameters should we fill in for those currently missing? How should we decide?
- How can we support customization without making it too easy for attackers to disable these supports for victims?
- What constraints should we be aware of that we haven’t already accounted for?
- Are there any missing attacks, scenarios, constraints or requirements?
- Where should these requirements be situated? (In the threat model document or elsewhere?)