Document 4: DULT Overall 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 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

- Our document aims to contribute to the following DULT WG goals:
  - Threat analysis
  - Documentation of the current state of tracker accessory platforms (Goal 1)
  - Standards-track protocol and guidance for preventing unwanted tracking (Goals 2, 3, 4)

Definitions

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

Attacker Taxonomy

- Expertise level
  - Expert: The attacker works in or is actively studying computer science, networking, computer applications, IT, or another technical field.
  - Non-expert: The attacker does not work or study in, or is a novice in, a technical field.
- Proximity to victim
  - High: Lives with victim or has easy physical access to victim and/or victim's possessions.
  - Medium: Has some physical access to the person and possessions of someone who lives with victim, such as when the attacker and victim are co-parenting a child.
  - Low: Does not live with or have physical access to victim and/or victim's possessions.
- Access to resources
  - High: The attacker has access to resources that may amplify the impact of other characteristics (e.g. significant finances, assistance, privileged access to technology).
  - Low: The attacker has access to few or no such resources.

Victim Taxonomy

- Expertise level
  - Expert: The victim works in or is actively studying computer science, networking, computer applications, IT, or another technical field.
  - Non-expert: The victim does not work or study in, or is a novice in, a technical field.
- Access to resources
  - High: The victim is generally able to safely access practical and relevant resources such as funds to pay a car mechanic, legal assistance, or other resources.
  - Low: The victim is generally unable to safely access practical and relevant resources.
- Access to technological safeguards
  - High: The victim is able to safely use, and has access to, technological safeguards such as active scanning apps.
  - Limited: The victim is able to safely use, and has access to, technological safeguards such as active scanning apps, but is unable to use their full capacity.
  - Low: The victim is not able to use technological safeguards such as active scanning apps, due to reasons of safety or access.

Tracking Tag Usage Taxonomy

- Attacker only: The attacker controls one or more tracking tags, but the victim does not.
- Victim only: The victim controls one or more tracking tags, but the attacker does not.
- Attacker and victim: Both the attacker and victim control one or more tracking tags.

Example Scenarios

Please see the example scenarios in Document 4 or the previous presentation from IETF 119.

What (we propose) is in scope for DULT WG

- 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

- 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. custom or altered tracking tags that bypass safeguards
  - Jailbreaking of a victim’s device
- Victim Profiles
  - N/A

Design Considerations

- 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