Detecting Unwanted Location Trackers
Internet-Draft
Intended status: Informational
Expires: 20 April 2026

M. Delano
Swarthmore College
J. Lowell
National Network to End Domestic Violence
S. Prabhu
Nokia
17 October 2025

DULT Threat Model
draft-ietf-dult-threat-model-03

Abstract

Lightweight Location-tracking Tags are in wide use to allow users to locate items. These Tags function as a component of a Crowdsourced Network in which Devices belonging to other network users (e.g., phones) report which Tags they see and their location, thus allowing the Owner(s) of the Tag to determine where their Tag was most recently seen. While there are many legitimate uses of these Tags, they are also susceptible to misuse for the purpose of stalking and abuse. A protocol that allows others to detect Unwanted Tracking must incorporate an understanding of the Unwanted Tracking landscape today. This document provides a threat analysis for this purpose, including a taxonomy of Unwanted Tracking and potential attacks against Detection of Unwanted Location Tracking (DULT) protocols. The document defines what is in and out of scope for the Unwanted Tracking protocols, and provides design requirements, constraints, and considerations for implementation of protocols to detect Unwanted Tracking.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://ietf-wg-dult.github.io/threat-model/draft-ietf-dult-threat-model.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-dult-threat-model/.

Discussion of this document takes place on the Detecting Unwanted Location Trackers Working Group mailing list (mailto:unwanted-trackers@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/unwanted-trackers/. Subscribe at https://www.ietf.org/mailman/listinfo/unwanted-trackers/.

Source for this draft and an issue tracker can be found at https://github.com/ietf-wg-dult/draft-ietf-dult-threat-model.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Location-tracking Tags allow users to locate items. These Tags function as a component of a Crowdsourced Network in which Devices belonging to other network users (e.g. phones) report on the location of Tags they have seen. At a high level, this works as follows:

* Tags ("Accessories") transmit a Location-enabled Advertisement Payload containing Accessory-specific information. The Payload indicates whether the Accessory is separated from its Owner(s) and thus potentially lost.

* Devices belonging to other users ("Non-Owner Devices") observe those Payloads and if the Payload is in a separated mode, report its location to a Crowdsourced Network.

* The Owner(s) queries the Crowdsourced Network for the location of their Accessory.

A naive implementation of this design exposes both a Tag’s user and anyone who might be targeted for location tracking by a Tag’s user, to considerable privacy risk. In particular:

* If Accessories simply have a fixed identifier that is reported back to the Crowdsourced Network, then the central server is able to track any Accessory without the user’s assistance.

* Any Attacker who can guess a Tag ID can query the Crowdsourced Network for its location.

* An Attacker can surreptitiously plant an Accessory on a Target and thus track them by tracking their "own" Accessory.

* Attackers could launch Denial-of-Service (DoS) attacks by flooding the Crowdsourced Network with spoofed Tag reports, disrupting real updates and overwhelming the Network.

* Frequent co-location of multiple Tags enables the Crowdsourced Network or a passive observer to infer social relationships, routines, or group behaviors, compromising user privacy without consent.

Detecting Unwanted Tracking is currently left to individual Tag manufacturers and Platforms on Non-Owner Devices. Each manufacturer and Platform has different implementations to prevent Unwanted Tracking, which may or may not be compatible with other manufacturers or Platforms. The goal of the IETF Detecting Unwanted Location Tracking (DULT) working group is to standardize a protocol between Location-tracking Tags, Non-Owner Devices, and Crowdsourced Networks.

In order to standardize a protocol for detecting Unwanted Tracking, thus minimizing the privacy risks described above, it is necessary to analyze and be able to model different privacy threats. This document includes: 1) a taxonomy of Unwanted Tracking, 2) methods Attackers could use to circumvent the DULT Protocol, and 3) design considerations for implementing the DULT protocol. The taxonomy of Unwanted Tracking uses a flexible framework to provide analysis and modeling of different threat actors, as well as models of potential Targets based on their threat context. It defines how these Attacker and Target persona models can be combined into threat models. The section on methods to circumvent the DULT protocol includes a threat matrix and description of several different possible attack vectors. Finally, the design considerations section focuses on specific requirements and constraints for successfully detecting Unwanted Tracking, alerting users, and providing guidance on disabling Tags (if desired). This threat model document is intended to inform the work of the implementation of the DULT Protocol as described in [I-D.draft-ietf-dult-Accessory-protocol] and [I-D.draft-ietf-dult-finding]. The DULT Protocol is based on an earlier Internet Draft; see [I-D.draft-ledvina-apple-google-unwanted-trackers].

1.1. Applicability

While there are many types of technology that can be used for Location Tracking, it is infeasible to attempt to describe a threat analysis for each possible technology in this document. The threat model described here is likely not applicable to the following areas: app-based technologies such as parental monitoring apps that do not use Location-tracking Accessories, Internet of Things (IoT) Devices that are Easily Discoverable, connected cars, or user accounts for cloud services or social media. A notable exception to this is GPS trackers; see Section 3.3.2 for relevant information and recommendations.

This threat model is also more likely to be applicable in regions where the use of Location-tracking Tags is more prevalent. While Location-tracking Tags have existed for over a decade, they became especially widely-used in the Global North in the last several years as Crowdsourced Networks were deployed by major smart phone

manufacturers. However, due to their reliance on a high density of Non-Owner Devices for the network to be effective and the relative cost of Location-tracking Tags, Location-tracking Tag use in the Global South is typically limited to affluent communities. If the cost of Non-Owner Devices and Location-tracking Tags decrease, an uptick of Unwanted Tracking could also occur in contexts where it is currently infeasible. This threat-model does still attempt to consider possible regional differences in Location-tracking Tag use (such as differences between rural and urban use), and also the sometimes limited resources that may be available to Targets of Unwanted Tracking.

2. Conventions and Definitions

2.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2.2. Definitions

Accessory: any product intended to interface with a Platform to connect to a Crowdsourced Network through the means described in these documents.

Active Scanning: method(s) of Unwanted Tracking detection that involves a user initiated scan for nearby Accessories. Contrast with Passive Scanning.

Attacker: any individual, group, or organization that is attempting to engage in Unwanted Tracking and/or circumvention of the DULT Protocol.

Crowdsourced Network: a service that Platforms communicate with to share and retrieve location information of Accessories.

Disablement: the process of preventing a specific Location-tracking Accessory from communicating with the Crowdsourced Network. This could be through physical means (e.g. removing the battery) or via a command sent by a Platform to an Accessory (e.g. Remote Disablement).

Disablement Instructions: steps Non-Owner Device users can take to disable a Location-tracking Accessory suspected of Unwanted Tracking.

Device: Hardware that includes software for a Platform and that can connect to Accessories and one or more Crowdsourced Networks. Examples of Devices are phones, tablets, laptops, etc.

Detecting Unwanted Location Tracking (DULT) Protocol the protocol under development by the IETF DULT working Group to prevent Unwanted Location Tracking. This includes protocols for Accessories and the crowd sourced network, along with algorithms for detecting Unwanted Tracking.

Easily Discoverable: an Accessory that is larger than 30 cm in at least one dimension, larger than 18 cm x 13 cm in two of its dimensions, and/or larger than 250 cm^3 in three-dimensional space. Location-tracking Accessories that are not Easily Discoverable MUST adhere to the DULT protocol.

Location-enabled Advertisement Payload: the Bluetooth (BT) advertisement payload that is advertised when an Accessory has recently, is currently, or will in the future provide location updates to its Owner.

Location-enabled State: the state an Accessory is in where its location can be remotely viewed by its Owner.

Location-tracking Accessory: any Accessory that has location-tracking capabilities, including, but not limited to, crowdsourced location, GPS/GNSS location, WiFi location, cell location, etc., and provides the location information back to an Owner Device via a Crowdsourced Network using the internet, cellular connection, etc. Location-tracking Accessories that are Easily Discoverable MUST adhere to the DULT Protocol. Location-tracking Accessories may also be referred to as Location-tracking Tags.

Location-tracking Tag: a term that may be used interchangeably with Location-tracking Accessory.

Non-Owner Device: a Device that may connect to an Accessory but is not an Owner Device of that Accessory.

Owner: an individual that is in active control of and the primary user of an Owner Device. An Owner may be associated with one or more Accessories and/or Devices.

Owner Device: a Device that is associated with the Accessory and can retrieve the Accessory’s location by querying the Crowdsourced Network.

(Obfuscated) Owner Information: (obfuscated) contact information

for an Accessory Owner. When an Accessory is marked as lost, this should include a phone number and/or email address. Otherwise, the information should be obfuscated to ensure privacy of Owners in cases where Accessories are falsely suspected of Unwanted Tracking or an Attacker attempts to determine the Owner of an Accessory. The information should include no more than the last two digits of a phone number and/or an obfuscated email address with the first letter of the username and entity visible, as well as the entire extension (e.g., b*****@i****.com).

Passive Scanning: method(s) of Unwanted Tracking detection that are running in the background on all Devices and may trigger Unwanted Tracking Alerts. Contrast with Active Scanning.

Platform: Operating systems that communicate with Accessories.

Platform-compatible Method: a method of communication between the Platform and the Accessory/Accessory manufacturers to exchange information, including, but not limited to, BT GATT protocol, BT advertisement, HTTP, etc.

Remote Disablement: the process of preventing a specific Location-tracking Accessory from communicating with the Crowdsourced Network via a command sent by a Platform.

Unwanted (Location) Tracking (UT): undesired tracking of a person, their property, or their belongings by a Location-tracking Accessory.

Unwanted Tracking Alert: an alert notifying the user of the presence of an unrecognized Accessory that may be traveling with them over time that allows them to take various actions, including playing a sound on the Accessory if the Accessory is in Bluetooth Low Energy (BLE) range.

Unwanted Tracking Detection: algorithms that detect the presence of an unknown Accessory traveling with a person over time.

Target: a individual who an Attacker is attempting to track without their consent. A Target may or may not own a Location-tracking Accessory.

3. Security Considerations

Incorporation of this threat analysis into the DULT Protocol does not introduce any security risks not already inherent in the underlying Location-tracking Tag protocols.

3.1. Security Considerations Unique To Unwanted Location Tracking

In a situation involving interpersonal control, an Attacker may be more likely to have access to a Target's Device or passwords. The Attacker could have physical access to a mobile Device on which a tracking account app is installed, remote access through a web portal, or both. The risk of an Attacker accessing a Target's tracking account remotely can be mitigated, though not eliminated, through support for different forms of multi-factor authentication (including hardware keys, e.g. Yubikeys, as well as more traditional methods). While this can also be used to mitigate the risk posed by physical access, taking overt security measures while frequently in physical proximity to the Attacker may lead to the Attacker escalating their tactics of interpersonal control. Risk assessments and the weighing of tradeoffs in such situations are often highly individualized. The ability of a user to access a tracking account over a web portal illustrates the need to consider web app security as part of support for detecting Unwanted Tracking.

3.2. Balancing Privacy and Security

In order to avoid pitting the privacy of Tag Owners not engaged in Unwanted Tracking against the security/safety of Targets, the DULT Protocol must consider and balance the privacy and safety of different users of the Crowdsourced Network. Existing attempts to prevent Unwanted Tracking (i.e. where an Attacker uses their own Tag to track a Target without their consent) have been criticized as potentially making it easier for an Attacker to track a Target using the Target's own Tag. This can occur if Tags do not rotate identifiers frequently enough. However, Eldridge et al. have demonstrated (https://eprint.iacr.org/2023/1332.pdf) a technological solution that employs secret sharing and error correction coding that may preserve the privacy of Tag Owners without reducing the efficacy of detecting Unwanted Tracking.

3.2.1. Security against Unwanted Tracking for potential Targets

The DULT Protocol must make it possible for potential Targets to discover Unwanted Tracking across Accessory hardware and Platforms within a reasonable amount of time. It should aid the Target in determining the location and Owner of the Accessory while not providing a full name or contact information on demand (as the Tag may merely have been lost or otherwise coincidentally in proximity, and providing excessive information would violate the privacy of a non-malicious Tag Owner). This could potentially be done with obfuscation, such as showing a partially redacted email address or phone number (see Section 4.1.1.1).

3.2.2. Privacy for potential Targets against the use of security measures for further surveillance

The DULT Protocol must consider the threat vector of an Attacker with access to a Target's Tag-associated account. In one study of how intimate partners misuse technology Freed et al, 2018 (https://dl.acm.org/doi/pdf/10.1145/3173574.3174241), 72% of survivors reported being forced or coerced to share passwords with an abuser. 41% reported that a cohabiting abuser "went through" their Device while they were not looking, allowing the abuser to obtain saved account passwords in many cases. 67% reported that an abuser was able to "hack" into their accounts remotely. To prevent use of a Target's own Tag as a means of surveillance, the protocol should minimize information that can be accessed from a web interface associated with a user's Tag-linked account.

3.2.3. Privacy for unassociated Tag Owners

Any unassociated Tag Owner, whether an abuse/stalking survivor or not, could potentially be the Target of an attack leveraging the Target's own Tags. Survivors and activists for women's and LGBTQIA+ rights, and/or against intimate interpersonal violence, may face severe government surveillance, repression, and even imprisonment Amnesty International, 2025 (https://www.amnesty.org/en/latest/news/2025/03/iran-authorities-target-womens-rights-activists-with-arbitrary-arrest-flogging-and-death-penalty/), Human Rights Watch, 2020 (https://www.hrw.org/news/2020/03/18/kazakhstan-womens-day-activists-convicted), Ruiz-Navarro, 2015 (https://www.theguardian.com/global-development/2015/mar/18/honduras-women-gladys-lanza-feminism-human-rights). Broad issues of technological privacy, including privacy against government and corporate surveillance, affect many populations, including but not limited to human rights defenders, children, migrants, and LGBTQIA+ people. Some people in these categories may _also_ be survivors of abuse or stalking. The DULT Protocol must not eschew legitimate privacy interests of Tag Owners in the name of safety and security for Targets.

The same person may be a Target of both Unwanted Tracking via an Attacker's Tag, and surveillance via their own Tag, either at different times or simultaneously. The DULT Protocol should account for this scenario.

3.3. Taxonomy of Unwanted Tracking

To create a taxonomy of threat actors, we can borrow from Dev et al.'s Models of Applied Privacy (MAP) framework (https://dl.acm.org/doi/fullHtml/10.1145/3544548.3581484). This framework is intended for organizations and includes organizational threats and taxonomies of potential privacy harms. Therefore, it cannot be applied wholesale. However, its flexibility, general approach to personas, and other elements, are applicable or can be modified to fit the DULT context.

The characteristics of threat actors may be described as follows. This is not intended to be a full and definitive taxonomy, but an example of how existing persona modeling concepts can be applied and modified.

* 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 Target
  - High: Lives with Target or has easy physical access to Target and/or Target's possessions.
  - Medium: Has some physical access to the person and possessions of someone who lives with Target, such as when the Attacker and Target are co-parenting a child.
  - Low: Does not live with or have physical access to Target and/or Target's possessions.
* Access to resources
  - High: The Attacker has access to resources that may amplify the impact of other characteristics. These could include, but are not limited to, funds (or control over "shared" funds), persons assisting them in stalking behavior, or employment that provides privileged access to technology or individuals' personal information.
  - Low: The Attacker has access to few or no such resources.

In addition, the Target also has characteristics which influence the threat analysis. As with Attacker characteristics, these are not intended as a definitive taxonomy.

* Expertise level
  - Expert: The Target works in or is actively studying computer science, networking, computer applications, IT, or another technical field.
  - Non-expert: The Target does not work or study in, or is a novice in, a technical field.
* Expectation of Unwanted Tracking
  - Suspecting: The Target has reason to believe that Unwanted Tracking is a likely risk.
  - Unsuspecting: The Target has no particular reason to be concerned about Unwanted Tracking.
* Access to resources
  - High: The Target is generally able to safely access practical and relevant resources. These might include funds to pay a car mechanic or private investigator, law enforcement or legal assistance, or other resources.
  - Low: The Target is generally unable to safely access practical and relevant resources.
* Access to technological safeguards
  - High: The Target is able to safely use, and has access to, technological safeguards such as active scanning apps.
  - Limited: The Target 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 Target is not able to use technological safeguards such as active scanning apps, due to reasons of safety or access.

It is also appropriate to define who is using the Location-tracking Tags and incorporate this into a model. This is because if protocols overly deprioritize the privacy of tracking Tags' users, an Attacker could use a Target's own Tag to track them (see Section 3.2).

* Tracking Tag usage

  - Attacker only: The Attacker controls one or more Location-tracking Tags, but the Target does not.

  - Target only: The Target controls one or more Location-tracking Tags, but the Attacker does not.

  - Attacker and Target: Both the Attacker and Target control one or more Location-tracking Tags.

Any of the threat analyses above could be affected by placement of the Tag(s). For instance, a Tag could be placed on a Target's person, or in proximity to a Target but not on their person (e.g. a child's backpack).

* Tag placement

  - Tag on Target's person or immediate belongings: This attack vector allows an Attacker to track a Target in a fine-grained way. It is also more likely that this attack would trigger an alert from the Tag.

  - Tag(s) in proximity to Target but not on their person (e.g. child's backpack, car): While this is a less fine-grained attack, it may also be less likely to be discovered by the Target. A child may not realize the significance of an alert or know how to check for a Tag. A parent may not think to scan for such a Tag, or may have more difficulty finding a Tag in a complex location such as a car.

  - Tags nearby but not used for Unwanted Tracking (e.g. false positives by companions or on transit): While this is not an attack vector in its own right, repeated false positives may discourage a Target from treating alerts seriously.

  - Multiple Tags using multiple types of placement: This attack vector may trick a Target into believing that they have fully addressed the attack when they have not. It also allows for a diversity of monitoring types (e.g. monitoring the Target's precise location, monitoring a child's routine, monitoring car usage).

3.3.1. Example scenarios with analyses

The following scenarios are composite cases based upon reports from the field. They are intended to illustrate different angles of the problem. They are not only technological, but meant to provide realistic insights into the constraints of people being targeted through Location-Tracking Tags. There is no identifying information for any real person contained within them. In accordance with research on how designers understand personas (https://dl.acm.org/doi/10.1145/2207676.2208573), the characters are given non-human names without attributes such as gender or race.

The analysis of each scenario provides an example usage of the modeling framework described above. It includes a tracking Tag usage element for illustrative purposes. However, as discussed previously, this element becomes more or less relevant depending on protocol evolution. Note that once a given Attacker persona has been modeled, it could be recombined with a different Target persona, or vice versa, to model a different scenario. For example, a non-expert Target persona could be combined with both non-expert and expert Attacker personas.

3.3.1.1. Scenario 1

3.3.1.1.1. Narrative

Mango and Avocado have two young children. Mango, Avocado, and the children all use smartphones, but have no specialized technical knowledge. Mango left because Avocado was abusive. They were homeless for a month, and the children have been living with Avocado. They now have an apartment two towns away. They do not want Avocado to know where it is, but they do want to see the children. They and Avocado meet at a public playground. They get there early so that Avocado will not see which bus route they arrived on and keep playing with the children on the playground until after Avocado leaves, so that Avocado will not see which bus route they get on. Two days later, Avocado shows up at Mango’ s door, pounding on the door and shouting.

3.3.1.1.2. Analysis

In this case, the Attacker has planted a Tag on a child. Co-parenting after separation is common in cases of intimate partner violence where the former partners have a child together. Child visits can be an opportunity to introduce technology for purposes of stalking the Target.

Attacker Profile	Avocado
Expertise Level	Non-Expert
Proximity to Target	Medium
Access to Resources	Unknown, but can be presumed higher than Mango's due to Mango's recent homelessness

Table 1

Target Profile	Mango
Expertise Level	Non-Expert
Expectation of Unwanted Tracking	Suspecting
Access to Resources	Low
Access to Technological Safeguards	High

Table 2

Other Characteristics	Avocado and Mango
Accessory Usage	Attacker Only
Tag Placement	In Proximity (on child)

Table 3

3.3.1.2. Scenario 2

3.3.1.2.1. Narrative

Strawberry and Elderberry live together. Neither has any specialized technological knowledge. Strawberry has noticed that Elderberry has become excessively jealous every time they go to visit a friend by themselves, Elderberry accuses them of infidelity. To their alarm, over the last week, on multiple occasions, Elderberry has somehow known which friend they visited at any given time and has started to harass the friends. Strawberry eventually gets a notification that a

Tag is traveling with them, and thinks it may be in their car, but they cannot find it. They live in a car-dependent area and cannot visit friends without the car, and Elderberry controls all of the "family" money, so they cannot take the car to the mechanic without Elderberry knowing.

3.3.1.2.2. Analysis

Here, the Attacker and the Target are still cohabiting, and the Attacker is monitoring the Target's independent activities. This would allow the Attacker to know if, for instance, the Target went to a police station or a domestic violence agency. The Target has reason to think that they are being tracked, but they cannot find the Tag. This can happen if the sound emitted by the Tag is insufficiently loud, and is particularly a risk in a car, where seat cushions or other typical features of a car may provide sound insulation for a hidden Tag. The Target could benefit from having a mechanism to increase the volume of the sound emitted by the Tag. Another notable feature of this scenario is that because of the cohabitation, the Tag will spend most of the time in "near-Owner state" as defined by the proposed industry consortium specification (see [I-D.detecting-unwanted-location-trackers]). Tags do not provide alerts in near-Owner state to reduce false positives.

Attacker Profile	Elderberry
Expertise Level	Non-Expert
Proximity to Target	High
Access to Resources	High

Table 4

Target Profile	Strawberry
Expertise Level	Non-Expert
Expectation of Unwanted Tracking	Suspecting
Access to Resources	Low
Access to Technological Safeguards	Impaired (cannot hear alert sound)

Table 5

Other Characteristics	Elderberry and Strawberry
Accessory Usage	Attacker Only
Tag Placement	In Proximity (car)

Table 6

3.3.1.3. Scenario 3

3.3.1.3.1. Narrative

Lime and Lemon have been dating for two years. Lemon works for a tech company and often emphasizes how much more they know about technology than Lime, who works at a restaurant. Lemon insists on having access to Lime's computer and Android phone so that they can "make sure they are working well and that there are no dangerous apps." Lemon hits Lime when angry and has threatened to out Lime as gay to their conservative parents and report them to Immigration & Customs Enforcement if Lime "talks back." Lime met with an advocate at a local domestic violence program to talk about going to their shelter once a bed was available. The advocate did some safety planning with Lime, and mentioned that there is an app for Android that can scan for location Tags, but Lime did not feel safe installing this app because Lemon would see it. The next time Lime went to see the advocate, they chose a time when they knew Lemon had to be at work until late to make sure that Lemon did not follow them, but when Lemon got home from work they knew where Lime had been.

3.3.1.3.2. Analysis

This is a case involving a high-skill Attacker, with a large skill difference between Attacker and Target. This situation often arises in regions with a high concentration of technology industry workers. It also may be more common in ethnic-cultural communities with high representation in the technology industry. In this case the Target is also subject to a very high level of control from the Attacker due to their imbalances in technological skills and societal status, and is heavily constrained in their options as a result. It is unsafe for the Target to engage in active scanning, or to receive alerts on their phone. The Target might benefit from being able to log into an account on another phone or a computer and view logs of any recent alerts collected through passive scanning.

Attacker Profile	Lemon
Expertise Level	Expert
Proximity to Target	High
Access to Resources	High

Table 7

Target Profile	Lime
Expertise Level	Non-Expert
Expectation of Unwanted Tracking	Suspecting
Access to Resources	Low
Access to Technological Safeguards	Low

Table 8

Other Characteristics	Lemon and Lime
Accessory Usage	Attacker Only
Tag Placement	Unclear

Table 9

3.3.1.4. Scenario 4

3.3.1.4.1. Narrative

Banana is a social media influencer. Fig is one of Banana's followers, and has become increasingly obsessed with Banana. Banana has no technical background. Fig has no formal technical background, but does read some online forums. Banana keeps a Location-tracking Tag on their keyring to prevent loss or theft of their home and car keys. Fig learns, from reading an online forum, how to find leaked passwords in data breaches, and is able to find the password to the account associated with Banana's Tag. Using the Crowdsourced Network, Fig is able to find Banana's home address and track their location. Fig makes a plan to travel to Banana's home and approach them in person.

3.3.1.4.2. Analysis

This scenario differs from the previous ones in three major ways. First, it requires no physical proximity between the Attacker and the Target. Second, the Attacker, like nearly one in five stalkers (SPARC - Stalking Infographic, 2022) (https://www.stalkingawareness.org/wp-content/uploads/2022/04/General-Stalking-Infographic.pdf), is a stranger. Third, in this scenario the Accessory belongs to the Target rather than the Attacker. The Attacker was able to use OSINT learned from an online forum in order to gain remote access to the Target's Accessory.

Attacker Profile	Fig
Expertise Level	Non-Expert
Proximity to Target	Low
Access to Resources	Unknown

Table 10

Target Profile	Banana
Expertise Level	Non-Expert
Expectation of Unwanted Tracking	Unsuspecting
Access to Resources	Unknown
Access to Technological Safeguards	Unknown

Table 11

Other Characteristics	Fig and Banana
Accessory Usage	Target Only
Tag Placement	On Target

Table 12

3.3.1.5. Scenario 5

3.3.1.5.1. Narrative

Orange and Grapefruit are university students in computer science. They attend multiple classes together, and are acquainted but do not regularly socialize or live in the same dormitory. Both use Location-tracking Tags to avoid losing items, as do many students at the university. Grapefruit has become increasingly obsessed with Orange, though Orange does not realize it. Grapefruit places Location-tracking Tags in Orange’s backpack and car. Orange found the one in their backpack after receiving a notification, but was not

suspicious when Grapefruit said that they had dropped it. Orange has not used their car in a week and is unaware of the well-hidden Tag there. Grapefruit has created a new account to associate with their backup phone and plans to associate multiple Tags with it, in order to place them on other possessions of Orange's.

3.3.1.5.2. Analysis

In this scenario involving two technical students, the Attacker, like over 40% of stalkers (SPARC - Stalking Infographic, 2022) (https://www.stalkingawareness.org/wp-content/uploads/2022/04/General-Stalking-Infographic.pdf), is an acquaintance. Both Attacker and Target are familiar with and use tracking Accessories. The Attacker is using multiple Accessories with a plan to incorporate more into their strategy.

Attacker Profile	Grapefruit
Expertise Level	Expert
Proximity to Target	Medium
Access to Resources	High

Table 13

Target Profile	Orange
Expertise Level	Expert
Expectation of Unwanted Tracking	Unsuspecting
Access to Resources	High
Access to Technological Safeguards	High

Table 14

Other Characteristics	Fig and Banana
Accessory Usage	Attacker and Target
Tag Placement	Multiple Types

Table 15

3.3.2. Bluetooth vs. other technologies

The above taxonomy and threat analysis focus on Location-tracking Tags. They are protocol-independent; if a Tag were designed for use with a Crowdsourced Network using a technology other than Bluetooth, they would still apply. The key attributes are the functionalities and physical properties of the Accessory from the user's perspective: the Accessory must be small, not Easily Discoverable, and able to participate in a Crowdsourced Network. While many GPS based location trackers are not explicitly designed for crowdsourced location-tracking, relying instead on cellular or satellite transmission, they offer different affordances that can have a critical impact on safety, including increased location precision and real-time tracking. Manufacturers of these trackers are strongly encouraged to add Bluetooth crowdsourced functionality so that DULT Protocols can be supported by GPS trackers.

3.4. Possible Attacks on the DULT Protocol

There are several different ways an Attacker could attempt to circumvent the DULT Protocol in order to track a Target without their consent or otherwise take advantage of the Crowdsourced Network. These include deploying multiple Tags to follow a single Target, using non-conformant Accessories and/or Devices, and taking advantage of possible differences between Crowdsourced Network implementations. This section includes a threat prioritization framework that assesses the risk of these attacks and how these risks may be mitigated.

3.4.1. Threat Prioritization Framework for DULT Threat Model

Threats in the DULT ecosystem vary in severity, feasibility, and likelihood, affecting users in different ways. Some threats enable long-term tracking, while others exploit gaps in detection mechanisms or leverage non-conformant Accessories and Devices. To assess and prioritize these risks, the following framework classifies threats based on their scope, impact, likelihood, risk level, affected users, and the availability of mitigations. A Threat Matrix is included that provides a structured assessment of known threats and their

associated risks. This categorization helps in understanding the challenges posed by different tracking techniques and their potential mitigations. While each attack included in this section only includes one value for potential impact, likelihood and risk level, in practice these values could differ depending on considerations discussed in Section 3.3 such as the proximity of the Attacker to the Target.

3.4.2. Threat Matrix

To systematically assess the risks associated with different threats, we introduce the following threat matrix. This categorization considers the following factors:

* Scope: The DULT WG document(s) most relevant to the attack.
  - Accessory: The Accessory protocol document, which describes the DULT Non-Owner Device protocol and other requirements for Accessories.
  - Finding: The finding algorithm document, which describes the DULT algorithm(s) to be implemented by Platforms/Devices.
  - Network: The Crowdsourced Network document, which describes the architecture of the Crowdsourced Network and includes guidance for Platforms/Devices.
* Impact: The potential consequences of the threat if successfully executed.
  - Low: Minimal effect on privacy and security.
  - Medium: Moderate effect on user privacy or tracking protection.
  - High: Severe privacy violations or safety risks.
* Likelihood: The probability of encountering this threat in real-world scenarios. This includes both the frequency of the attack and how easy it is to execute.
  - Low: Rare or requires specific conditions and high technical effort.
  - Medium: Possible under common scenarios with moderate technical requirements.
  - High: Frequently occurring or easily executed using common tools or skills.

* Risk Level: A qualitative assessment based on impact and likelihood.
  - Low: Limited risk requiring minimal mitigation.
  - Medium: Requires mitigation to prevent common attacks.
  - High: Critical threat must be addressed.
* Affected Users: These are categorized as either:
  - Targets: Individuals specifically targeted for the purposes of Unwanted Tracking.
  - All users: Anyone using the system, even if they are not directly targeted.
* Mitigation Available?: Whether a known mitigation strategy exists.
  - Yes: A viable mitigation exists.
  - Partial: Some mitigations exist, but are not fully effective.
  - No: No effective mitigation currently available.

Threat	Scope	Impact	Likelihood	Risk Level	Affected Users	Mitigation Available?
Deploying Multiple Tags	Finding	Medium	High	High	Targets	Yes
Remote Advertisement Monitoring	Accessory, Network	Medium	High	Medium	All users	Partial
Physically Modifying Tags	Accessory	High	Medium	Medium	Targets	Partial
Accessory Firmware Modifications	Accessory	High	Low	Medium	Targets	Partial
Attacker Accessory Disablement	Accessory, Finding	Medium	Medium	Medium	Targets	Partial

Tracking Using Target's Own Tag	Network	High	Medium	High	Targets	Partial
Disabling Target Tag Detection	Network	High	Medium	Medium	Targets	Partial
Disabling Target Tag	Accessory, Network	Medium	Medium	Medium	Targets	Partial
Impersonation Attack (Tag)	Accessory, Finding, Network	High	Medium	High	Targets	Partial
Impersonation Attack (Device/Tag)	Accessory, Network	High	Medium	High	All users	Partial
Impersonation Attack (Device/ Network)	Network	Medium	Low	Low	All users	Partial
Replay Attack	Accessory, Network	Medium	High	Medium	All users	Partial
Heterogeneous Tracker Networks	Accessory, Finding, Network	High	Medium	Medium	Targets	No
Deploying GPS Tracker	Accessory	High	Medium	High	Targets	Partial

Table 16

3.4.3. Deploying Multiple Tags (Finding)

When an Attacker deploys Location-tracking Tags to follow a Target, they may deploy more than one Tag. For example, if planting a tracking Tag in a car, the Attacker might place one Tag inside the car, and another affixed on the outside of the car. The DULT Protocol must be robust to this scenario. This means that scans, whether passive or active, need to be able to return more than one result if a Tag is suspected of being used for Unwanted Tracking, and the time to do so must not be significantly impeded by the presence

of multiple Tags. This also applies to situations where many Tags are present, even if they are not being used for Unwanted Tracking, such as a busy train station or airport where Tag Owners may or may not be in proximity to their Location-tracking Tags. Instead of distributing multiple Tags in the same location, an Attacker could also distribute multiple Location-tracking Tags across locations frequently visited by a Target (home, workplace, etc.).

The impact of this attack is medium for typical cases involving a small number of Tags, though the impact could escalate if an Attacker deploys dozens of Tags. The likelihood is high, as deploying multiple Tags requires minimal technical effort and can be done using inexpensive, commercially available Tags, making the attack easily repeatable. As a result, the overall risk is high, requiring robust countermeasures. The impact of multiple Tags can be fully mitigated by scanning for multiple Tags, though a sophisticated Attacker might deploy other techniques such as modifying Tag firmware (Section 3.4.6) or periodically disabling a Tag (Section 3.4.7) to evade detection.

3.4.4. Remote Advertisement Monitoring (Accessory, Network)

Any Device with Bluetooth scanning capabilities in proximity to a Location-tracking Tag can receive Bluetooth advertisement packets. If an Attacker is able to link an identifier in an advertisement packet to a particular Tag, they may be able to use this information to track the Tag over time, and by proxy the Target or other individual, without their consent.

The impact of remote advertisement monitoring is moderate, as tracking generally compromises privacy but, in many cases, prolonged observation primarily reveals the location of the object rather than of the person. The likelihood is high, as Attackers can execute this using off-the-shelf Bluetooth scanning tools or smartphone apps with minimal technical knowledge. As a result, this is classified as a medium risk attack. This attack can be partially mitigated by rotating tracking identifiers.

Tracking Tags typically rotate any identifiers associated with the Tag, with the interval depending on context: when near the Owner’s Device, identifiers rotate frequently (every 1530 minutes), while in a separated state, rotation may occur only once every 24 hours (see [I-D.detecting-unwanted-location-trackers]). Eldridge et al. have demonstrated (https://eprint.iacr.org/2023/1332.pdf) a technological solution that employs secret sharing and error correction coding that would reduce this to 60 seconds. However, work must investigate how robust this scheme is to the presence of multiple Tags (see Section 3.4.3).

While rotating identifiers provides partial mitigation, Attackers can still use advanced correlation techniques, such as signal fingerprinting, timing analysis, and multi-sensor triangulation, to bypass this defense. These methods leverage unique transmission characteristics, RSSI (Received Signal Strength Indicator) variations, and environmental factors to probabilistically link rotating identifiers back to a single Tag over time. Prior research, such as Eldridge et al., has demonstrated (https://eprint.iacr.org/2023/1332.pdf) how statistical models can be used to correlate Bluetooth signals even when identifiers change frequently. Additional work by Despres et al. further demonstrates (https://people.eecs.berkeley.edu/~daw/papers/deTagtive-snip23.pdf) that BLE Accessories using rotating identifiers can be deanonymized through RSSI-based correlation techniques.

3.4.5. Physically Modifying Tags (Accessory)

An Attacker might physically modify a Tag in ways that make it non-conformant with the DULT Protocol. Physical modifications may include disabling a speaker or other haptics, or shielding and altering the antenna to reduce transmission range. These modifications can make it more difficult for Victims to discover hidden Tags, leading to a high impact. The likelihood is medium, as such hardware modifications require moderate technical expertise and physical access to the Tag. Given this combination of factors, the overall risk level is medium. Partial mitigation is available, such as monitoring the impedance of the speaker, but these mitigations are limited as Attackers have physical access to the Tags.

3.4.6. Accessory Firmware Modifications (Accessory)

The DULT Protocol (see [I-D.draft-ietf-dult-Accessory-protocol]) will specify that Accessory firmware images MUST be authenticated, and that Accessories MUST verify the integrity and origin of firmware. However, if these protections were to be bypassed, an Accessory’s firmware could be altered to deviate from standard behavior. Attackers may manipulate advertisement intervals to reduce detection opportunities, allowing the Tag to evade tracking for extended periods, or rotate IDs rapidly, disrupting detection systems that rely on tracking unknown Accessory persistence.

Firmware-based changes would have high impact. The likelihood is low, as these attacks require significant technical expertise to bypass firmware verification and modify low-level Accessory behavior. As a result, the overall risk level is medium. Partial mitigation of this attack is possible by requiring Accessories to verify the integrity and origin of firmware.

3.4.7. Attacker Accessory Disablement (Accessory, Finding)

An Attacker might intentionally disable their Location-tracking Tag to make it harder for a Victim to detect and/or locate the Tag. This could be done periodically or permanently and either remotely or using a physical device (https://undetecTag.com/products/undetecTag).

The likelihood is medium, as this attack is relatively easy to perform using commercially available tools, but it still requires some Attacker awareness of the Target's actions (e.g., an ongoing search). The impact is medium as the Tag can still be detected and physically located, though it may be more difficult to do so. The risk level is medium. The impact of this attack can be partially mitigated by minimizing the time needed to detect Unwanted Tracking and maintaining the same identifier on reset.

3.4.8. Tracking Using Target's Own Tag (Network)

Attackers with access to a Target's account, either through password reuse, phishing, social engineering, or credential theft, can exploit DULT's Ownership model by using the Target's own Tag to monitor their location. Since the Tag is registered to the Target, the system assumes the user is the legitimate Owner and suppresses any Unwanted Tracking alerts. This creates a significant blind spot, as the Target is effectively tracked by their own Tag without any warning.

This threat differs from impersonation or replay attacks (see Section 3.4.11 and Section 3.4.13) because it does not rely on breaking cryptographic protections or evading detection algorithms. Instead, it leverages the legitimate trust relationship encoded in the protocol. The impact of this attack is high, as it results in silent tracking with no alert mechanism. The likelihood is medium, as account compromise is a relatively common occurrence in real-world settings, though it still requires some Attacker effort or opportunity. Overall, the risk level is high due to the complete circumvention of core notification systems.

Partial mitigation may be possible through account activity monitoring, anomaly detection (e.g., login from unfamiliar location or Device), and notifications of significant account events (such as Tag access or Tag movement linked to a different Device). However, these features depend on Platform implementation and may not be uniformly enforced.

3.4.9. Disabling Target Tag Detection (Network)

An Attacker might intentionally disable passive Unwanted Tracking detection on a Target's Device.

The impact of this attack is high as it would prevent the Target from being notified about possible Unwanted Tracking. The likelihood is medium, as executing this attack requires the Attacker to physically or remotely alter settings on the Target's Device, which involves moderate effort and access. The risk level is medium. This attack can be partially mitigated by notifying Targets of potential location tracking using other means e.g. sounds or haptics on Location-tracking Tags.

3.4.10. Disabling Target Tag (Accessory, Network)

An Attacker might intentionally disable a Target's Tag as a form of harassment. This could be done with physical access to the Tag, using a Target's own Device to disable the Tag, or with remote access to disable the Tag via the Crowdsourced Network. The impact of this attack is medium as it is a nuisance but most likely does not involve a security threat, unless the Tag is being used to track a valuable item or child. The likelihood is medium, as executing the attack requires access to the Target's Tag, Device, or account, which involves a moderate level of access or effort. The risk level is therefore medium. Physical disablement of a Tag cannot be mitigated, but other forms of disablement may be mitigated by notifying users that a change has been made on their account, similar to suspicious login notifications.

3.4.11. Impersonation Attack (Tag; Accessory, Finding, Network)

Attackers might be able to impersonate legitimate tracking Accessories, enabling tracking without complying with the DULT Protocol. This can be done by deploying custom Tags (https://www.hackster.io/news/fabian-braunlein-s-esp32-powered-find-you-Tag-bypasses-apple-s-airTag-anti-stalking-protections-0f2c9ee7da74) or by using Devices to mimic Tags (https://cec.gmu.edu/news/2025-02/find-my-hacker-how-apples-network-can-be-potential-tracking-tool). By impersonating an authorized Tag, an Attacker could inject false location data, misattribute Tag Ownership, or evade detection by appearing as a trusted Accessory or rotating identifiers frequently. This tactic increases the difficulty of accurately identifying unauthorized tracking attempts and undermines the reliability of the network.

In addition to full impersonation, adversaries may exploit Platform-specific assumptions to suppress alerts. For instance, Chen et al. describe (https://www.usenix.org/system/files/conference/usenixsecurity25/sec25cycle1-prepub-1266-chen-junming.pdf) a technique in which an Attacker sets the status field of a broadcast message to 0x00 to emulate MacBook location beacons. Since such beacons are typically

ignored by Apple’ s Unwanted Tracking alerts, this evasion method allows the Attacker to remain undetected. This demonstrates how Attackers can exploit trust assumptions about certain Accessory classes to bypass user protections, further complicating detection and mitigation.

The impact of this attack is high, as it enables real-time location tracking by exploiting the behavior of the Crowdsourced Network. The likelihood is medium, as the attack requires deploying custom hardware or exploiting Platform-specific capabilities like unrestricted Bluetooth broadcasting, which have been demonstrated in research but remain moderately complex to execute. As a result, the overall risk level is considered high. Currently, no fully effective mitigation exists. However, improvements in authentication mechanisms, such as cryptographic signing of broadcasts, and anomaly detection techniques may help reduce the risk. Protocol-level authentication is needed to validate Accessory identities and prevent these attacks. Operating systems can partially mitigate software impersonation attacks by restricting low-level BLE broadcasting unless elevated privileges are granted.

3.4.12. Impersonation Attack (Device)

In addition to impersonating a Tag, an Attacker could also impersonate a Device. This affords attacks against both Accessories and against the Crowdsourced Network.

3.4.12.1. Attacks on Accessories (Accessory, Network)

An impersonated Device could send commands to Accessories, such as a "play sound" command or a remote disablement command. Accessory firmware should either attempt to verify the authenticity of commands from Devices or otherwise limit how Accessories respond to commands from Devices. For example, Accessories that receive a "play sound" command from a Non-Owner Device should only execute the command if the Accessory is away from its Owner. Similarly, Accessories should only respond to remote disablement commands if the Accessory can reasonably be expected to be used for Unwanted Tracking and the Accessory can confirm that a Device has used other finding techniques to locate the Accessory.

The impact of a Device impersonation attack is high if it is able to send arbitrary commands to Accessories. The likelihood of such an attack is medium as it can be done by any Device able to transmit BTLE packets but requires some familiarity with the DULT Protocol. Therefore, the overall risk level is high. The affected users are all users. Mitigation is partial; while Devices cannot be prevented from transmitting packets, certain rules can be enforced by Accessories.

3.4.12.2. Attacks on Crowdsourced Network (Network)

An impersonated Device could send false location reports to the Crowdsourced Network, or selectively not report to the Crowdsourced Network.

The likelihood of this attack is low, as it would require the impersonated Device to authenticate with the Crowdsourced Network. The impact is medium, as not reporting would have negligible impact and false location reports are a nuisance but can be mitigated. The overall risk level for this attack is low. The affected users are all users. Mitigations include requiring authentication to send reports to the Crowdsourced Network and only trusting reports when they can be verified by multiple Devices.

3.4.13. Replay Attack (Accessory, Network)

In addition to impersonating legitimate Accessories (see Section 3.4.11), Attackers can record and replay Bluetooth advertisements from a legitimate Accessory. For example, an Attacker could capture an Accessory’s broadcast and retransmit it elsewhere, creating confusion about its actual location. This could be used to mislead users, interfere with tracking accuracy, or frame an innocent party by making it appear as though they are carrying an Accessory or in a location when they are not.

The impact of this attack is medium. The likelihood is high, as replay attacks require no authentication and can be executed using off-the-shelf Bluetooth scanning tools with minimal technical expertise. Replay attacks pose a medium risk owing to their higher likelihood but medium impact. Replay attacks are particularly difficult to mitigate as they may involve different combinations of Accessories and Devices. Partial mitigation may be possible by authenticating messages from Accessories in a time varying manner.

3.4.14. Heterogeneous Tag Networks (Accessory, Finding, Network)

Attackers may use a mix of Tags from different manufacturers (e.g., Apple AirTags, Tile, Samsung SmartTags) to exploit gaps in vendor-specific tracking protections. Many detection systems are brand-dependent, making them ineffective against mixed Tag deployments. The goal of the DULT Protocol is to enable a cross-vendor framework; however, any slight differences in implementation could be exploited.

The impact is high, as it circumvents traditional defenses. The likelihood is medium, as deploying or selecting from multiple brands requires effort and coordination, and may demand deeper knowledge of Platform-specific behaviors and limitations. Overall, this is medium risk attack. This attack can be mitigated by manufacturers adopting the DULT Protocol and ensuring that the DULT Protocol is sufficiently clear to minimize gaps in vendor-specific tracking protections.

3.4.15. Deploying GPS Tracker (Accessory)

When an Attacker deploys a GPS tracker to stalk a Target, they have access to greater location precision, real-time tracking, and even global coverage through satellite connection for some trackers. Attackers are especially likely to use GPS trackers in rural areas and areas with low Crowdsourced Network saturation, or when looking for more advanced precision or for Accessories that do not offer safety protections.

The impact of this attack is high due to the increased location precision and real-time tracking functionality. The likelihood is medium, as these trackers are currently more expensive than Bluetooth based trackers, and not as readily available. As a result, the overall risk is high, requiring robust countermeasures. The impact of GPS trackers can be mitigated by adding Bluetooth crowdsourced location-tracking functionality to GPS trackers and adopting the DULT Protocol. However, the adoption of the DULT Protocol by GPS tracker manufacturers is of course optional, so this is considered a partial mitigation.

3.5. What is in scope

3.5.1. Technologies

The scope of this threat analysis includes any Accessory that is small and not Easily Discoverable and able to transmit its location to consumer Devices using Bluetooth. Larger and/or Easily Discoverable Accessories/Devices such as laptops with location-tracking integrations may also choose to implement the protocol.

3.5.2. Attacker Profiles

An Attacker who deploys any of the attacks described in Section 3.4.1 is considered in scope. This includes: Attackers who track Victims using a Location-tracking Tag and applications readily available for end-users (e.g. native tracking application), Attackers who physically modify Location-tracking Tags (e.g. to disable a speaker), and Attackers who make alterations to the firmware of an existing tracking Tag or create custom Tags that successfully connect to Devices and therefore the Crowdsourced Network.

3.5.3. Target Profiles

All Targets profiles are in scope regardless of their expertise, access to resources, or access to technological safeguards. For example, protocols should account for a Target’s lack of access to a smartphone, and scenarios in which Targets cannot install separate software.

4. Design Considerations

As discussed in Section 3, Unwanted Tracking can involve a variety of Attacker, Target, and Tag profiles. A successful implementation to preventing Unwanted Tracking should:

* 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 the scope defined in Section 3.5

* Account for scenarios in which the Target has low expertise, access to resources, and/or access to technological safeguards within the scope defined in Section 3.5

* Avoid privacy compromises for Tag Owner(s) when protecting against Unwanted Tracking. The privacy of Tag Owner(s) and the security of Targets should be considered equally.

4.1. Design Requirements

The DULT Protocol should 1) allow Targets to detect Unwanted Tracking, 2) help Targets find Tags that are tracking them while minimizing false positives (e.g., avoiding legitimate, co-owned, or nearby Tags being misidentified as threats), and 3) provide instructions for Targets to disable those Tags if they choose. These affordances should be implemented while considering the appropriate

privacy and security requirements.

4.1.1. Detecting Unwanted Location Tracking

There are four ways that the DULT Protocol should assist Targets in detecting potentially Unwanted Tracking: 1) active scanning, 2) passive scanning, 3) tracking Tag alerts, and 4) Crowdsourced Network activities logs.

4.1.1.1. Active Scanning

There may be scenarios where a Target suspects that they are being tracked without their consent. Active scanning should allow a user to use a native application on their Device to search for Location-tracking Tags that are separated from their Owners. When a Tag has been identified as potentially being used for Unwanted Tracking, the user should be able to view the serial number of the Device along with Obfuscated Owner Information and instructions on how to find and/or disable the Tag (see Section 4.1.2 and Section 4.1.3). Additional information about when that Tag has been previously encountered within a designated time window (e.g. the last 12 hours) should also be included if available (see Section 3.2). Allowing users to "snooze" or ignore Tags known to be safe (e.g. Tags from a family member) could also be implemented. Tracking Tags that are near their Owners should not be shared to avoid abuse of the active scanning feature.

4.1.1.2. Passive Scanning

Platforms should passively scan for Tags suspected of Unwanted Tracking and notify the user. This will involve implementing one or more algorithms to use to flag Tags and determine when to notify the user. (A dedicated DULT WG document will address tracking algorithms, and will be linked when it is available.) The user could be notified through a push notification or through Sounds and Haptics (see Section 4.1.1.3). When a Tag has been identified as potentially being used for Unwanted Tracking, the user should be able to view the serial number of the Tag along with Obfuscated Owner Information for all accounts linked to the Tag and instructions on how to find and/or disable the Tag (see Section 4.1.2 and Section 4.1.3). There will be tradeoffs between detecting potential Unwanted Tracking promptly and alerting the potential Target prematurely. One way to handle these tradeoffs is to allow users to set the sensitivity of these alerts. For example, the AirGuard (https://github.com/seemoo-lab/AirGuard) app includes three different "Security Level" settings that users can customize.

To improve the accuracy of Unwanted Tracking detection, a confidence scoring mechanism can be used. Instead of issuing binary alerts for all detected Tags, the system assigns a confidence score based on multiple factors, helping distinguish between genuine tracking threats and benign scenarios. This section outlines potential factors that may contribute to assessing the likelihood of Unwanted Tracking. Each factor can be considered independently to help inform an overall risk assessment. A confidence-based approach offers the following advantages:

* Reduced False Positives: A confidence-based approach can help filter out benign tracking scenarios, such as transient signals or shared family Tags. Instead of triggering alerts based solely on presence, the system can dynamically adjust its sensitivity based on behavioral patterns. For example, if a tracking Tag appears near a user only briefly or follows a predictable shared usage pattern (e.g., a Bluetooth Tag frequently used by family members), it may be assigned a low confidence score. This prevents unnecessary alerts while still ensuring that persistent and anomalous tracking behaviors are flagged for user attention.

* Context-Aware Threat Evaluation: The confidence score can incorporate contextual factors such as movement patterns, duration of proximity, and recurrence. For instance, if a Tag is detected only once in a public place (e.g., at a caf or airport), it is less likely to indicate malicious tracking. However, if the same Tag reappears near the user across multiple locations or over an extended period, its confidence score increases, prompting a higher-priority alert.

* Adaptive Alert Sensitivity: By dynamically adjusting detection thresholds based on confidence scores, the system can prioritize high-risk scenarios while minimizing unnecessary alerts. Users may receive warnings based on escalating levels of certainty, such as:

  - Low confidence: Informational notification (e.g., "An unfamiliar Tag was briefly detected nearby.")

  - Medium confidence: Warning with recommended actions (e.g., "A Tag has been detected multiple times near you. Check your surroundings.")

  - High confidence: Urgent alert with mitigation options (e.g., "A Tag has been persistently following you. Consider removing or disabling it.")

This approach ensures that users receive actionable and meaningful alerts, reducing notification fatigue while maintaining strong protection against Unwanted Tracking. The confidence scoring approach could include the variables listed below.

4.1.1.2.1. Duration of Proximity

Tracks how long a Tag remains in close proximity to the user.

Rationale: Tags that persist near a user for extended periods are more likely to indicate tracking activity than transient encounters (e.g., passing someone on public transit).

4.1.1.2.2. Movement Correlation

Measures how closely the movement of the suspected Tag mirrors that of the user.

Rationale: High movement correlation (e.g., appearing at home, then work, then a store with the user) increases the likelihood that the Tag is following the user intentionally.

4.1.1.2.3. Signal Strength Trends

Observes how the signal strength of the suspected Tag (e.g., Bluetooth RSSI) changes over time.

Rationale: A sustained or increasing signal strength suggests physical proximity to the user, strengthening the case for intentional tracking.

4.1.1.2.4. Persistence

Evaluates how often and across how many different times/locations the same Tag is observed, while accounting for identifier rotation.

Rationale: Frequent reappearances over time and space can indicate deliberate placement, even if identifiers change periodically.

4.1.1.2.5. Hardware Identity

Analyzes available Bluetooth advertisement metadata, such as vendor-specific fields or Tag model indicators, while respecting identifier randomization.

Rationale: Certain Tags (e.g., known commercial Tags) are more likely to be associated with tracking. Even with rotating identifiers, consistent vendor metadata or other characteristics may provide useful signals.

4.1.1.2.6. Environmental Context

Considers the location in which the Tag is seen (e.g., home, office, public places).

Rationale: Tags seen only in familiar, safe zones may be harmless. Appearances in unfamiliar or private locations without explanation raise concern.

4.1.1.3. Location-tracking Tag Alerts

Location-tracking Tags may be difficult to locate, and users may not have a Device that can actively or passively scan for Location-tracking Tags. The DULT Protocol should be built with accessibility in mind (https://cdt.org/insights/centering-disability-in-mitigating-harms-of-bluetooth-tracking-technology/) so that the most people can be protected by the protocol. In addition to push notifications on nearby Devices, Location-tracking Tags themselves should be able to notify end users. This should include periodic sounds when away from all Tag Owners, along with lights and haptics so that people who are Deaf or hard of hearing can still locate them. Tracking Tag Alerts should also educate the user on methods to successfully find and disable Tags (see Section 4.1.2 and Section 4.1.3).

4.1.1.4. Crowdsourced Network Activities Logs

Stephenson et al. (https://www.usenix.org/system/files/usenixsecurity23-stephenson-lessons.pdf) point out that Internet of Things devices like Location-tracking Accessories do not have ways to reveal abusive behavior. This can be addressed through the use of detailed logs that provide insights for Victims about which accounts have accessed the location of which Accessories and when. Crowdsourced Networks should log common user activities for review by each Accessory Owner, and should not be able to be easily deleted by Accessory Owners, who might do so as a way to hide evidence of Unwanted Tracking.

Logs should include sufficient detail to detect Unwanted Tracking without being another vector for surveillance. For example, a log could state that "User B viewed the location of Accessory X at [time]." By including information about user, Accessory, and time, Victims can determine whether their own Accessories are being used to track them, and whether or not their accounts connected to the Crowdsourced Network are compromised.

4.1.2. Finding Tracking Tags

Even after a Tag is detected through passive or active scanning, a user may have difficulty in locating it. For example, a Tag may be buried under a vehicle cushion. Platforms should allow users who have discovered a Tag through passive or active scanning to request that the Tag signal its presence. This assistance should be done in a way that is accessible to users with sensory or other impairments by using multimodal signals as described in Section 4.1.1.3. Manufacturers/Platforms may also implement other methods to assist in locating Tags, such as precision finding using Ultra-wideband.

4.1.2.1. Lost Mode

Some Platforms allow Accessories to be marked as lost. When another user finds the Accessory, they can view a message and/or contact information of the Accessory Owner. While helpful in a benign case where an Accessory is truly lost, care must be taken to ensure that the lost mode function is not used for harassment. Platforms should use a non-customizable lost message and display either Obfuscated Owner information, or a full phone number or email address if the Accessory Owner chooses to share that information.

4.1.3. Disabling Tracking Tags

In order to effectively prevent Unwanted Tracking, users should be able to disable Location-tracking Tags. This includes a Non-Owner user being tracked by a Tag’s Owner, as well as an Owner user who believes that an Attacker is using their own Tag to track them. Platforms should provide instructions for disabling Location-tracking Tags once they are located. Manufactures/Platforms should also consider allowing Location-tracking Tags to be disabled remotely.

Beyond simple deactivation, users should also receive guidance on additional steps they may take, depending on their specific situation:

* Advice on destruction or preservation: In some cases, destroying a Tag may eliminate the risk of further tracking. However, users should be made aware that doing so may result in the loss of

evidence that could otherwise be used to prove tracking or identify an abuser. Destroying the Tag might also lead to escalation in abusive contexts. Guidance should help users weigh these risks and determine the most appropriate course of action.

* Serial number access and use: Platforms should inform users how to retrieve the serial number or unique identifier of the Tag, even if the Tag is not from the same Platform. Serial numbers may be used to report the Tag, verify its origin, or, in cooperation with manufacturers or authorities, identify the registered Owner(s) of the Tag.

It is important to consider where educational and disabling guidance is hosted. For instance, information about disabling Tags should be publicly accessible, possibly from neutral, decentralized, or international organizations, to mitigate the risk of government censorship or politically motivated takedowns. This ensures access for vulnerable users, including those in high-risk environments or authoritarian regions.

4.1.4. Notification Management for Trusted Accessories

To reduce alert fatigue and improve user experience, implementations should allow users to snooze passive notifications from Location-tracking Tags that have been explicitly marked as trusted or friendly. This is particularly useful in scenarios where users regularly encounter the same Tag (e.g., a family member’s keys or a shared vehicle Tag).

Such snoozed Tags may also be de-prioritized or grouped separately during active scans, helping users focus on unfamiliar or potentially malicious Tags. Platforms should make it easy to manage snoozed Tags and review or revoke trust status as needed. It is also advisable to implement revalidation mechanisms, for example, resuming notifications after a period of time to prevent long-term blind spots.

Some Platforms may wish to implement family sharing or shared Ownership models, where multiple users can be associated with a single Tag. However, this introduces the risk of abuse (e.g., an Attacker adding a Target to the shared list in order to avoid triggering passive notifications), and therefore should be approached with caution and abuse mitigation in mind. These features are optional and may vary by Platform. Whenever shared Ownership is used, information about all Owners should be made available when a Tag is suspected of Unwanted Tracking (see Section 4.1.1.2).

4.2. Design Constraints

There are also design constraints that the DULT Protocol must consider, including limitations of the Bluetooth Low Energy (BLE) protocol, power constraints, and Device constraints.

4.2.1. Bluetooth constraints

Detecting Tags requires analyzing Bluetooth Low Energy (BLE) advertisement packets. Advertisements are publicly transmitted, allowing passive scanning by any nearby receiver. While this enables open detection of unknown Tags, it also raises privacy concerns (see Section 1). Some BLE implementations employ randomized MAC addresses and other privacy-preserving techniques, which could impact persistent tracking detection.

The BLE payload in BLE 4.0 can support advertisement packets of up to 37 bytes. One current adoption of Unwanted Tracking detection requires 12 of these bytes for implementing the basic protocol, with the remaining optional (see [I-D.detecting-unwanted-location-trackers]). Implementation of the DULT Protocol will need to consider these limitations. For example, in Eldridge et al (https://eprint.iacr.org/2023/1332.pdf), implementing Multi-Dealer Secret Sharing required using two advertisement packets were needed instead of one due to payload constraints. While BLE 5.0 supports 255+ bytes of data, the protocol is not backwards compatible and thus may not be suitable for the DULT Protocol.

BLE advertisements operate in the 2.4 GHz ISM band, making them susceptible to interference from Wi-Fi, microwave ovens, and other wireless devices. The presence of environmental noise may degrade detection accuracy and introduce variability in scan results.

BLE uses channel hopping for advertising (three advertising channels). Scanners need to cover all these channels to avoid missing advertisements. The BLE protocol also enforces strict power efficiency mechanisms, such as advertising intervals and connection event scheduling, which impact detection frequency. Devices operating in low-power modes or sleep modes may significantly reduce their advertisement frequency to conserve energy, making periodic detection less reliable. Furthermore, Platform-level constraints, such as OS-imposed scanning limits and background activity restrictions, further impact the consistency and responsiveness of tracking detection mechanisms. For further discussion of power constraints, see Section 4.2.2.

Additionally, Bluetooth-based tracking systems typically rely on an active Bluetooth connection on the Owner’ s Device to determine whether a Tag is in the Owner’s possession. If the Owner disables Bluetooth on their phone, the system may incorrectly infer that the Tag is no longer nearby, potentially triggering a false positive alert for Unwanted Tracking. This limitation arises from the inability of Bluetooth-based systems to verify proximity without active signals from the Owner’ s Device. There is currently no straightforward solution to this issue using Bluetooth alone, and it represents an inherent trade-off between privacy and detection reliability. Systems should account for this possibility and communicate it clearly to users.

To address these challenges, detection mechanisms must balance efficiency, privacy, and accuracy while working within the constraints of the BLE protocol. Solutions may include leveraging multiple observations over time, integrating probabilistic risk scoring, and optimizing scanning strategies based on known BLE limitations.

4.2.2. Power constraints

Unwanted tracking detection mechanisms typically rely on periodic Bluetooth scanning to identify unknown Accessories. However, continuous background scanning poses a significant power challenge, especially for mobile Devices with limited battery capacity. Maintaining high-frequency scans for extended periods can lead to excessive energy consumption, impacting Device usability and battery longevity.

To address these concerns, detection systems must incorporate power-efficient approaches that balance security with practicality. Adaptive scanning strategies can dynamically adjust the scan frequency based on contextual risk levels. For example, if a suspicious Accessory is detected nearby, the system can temporarily increase scan frequency while reverting to a lower-power mode when no threats are present.

Event-triggered detection offers another alternative by activating scanning only in specific high-risk scenarios. Users moving into a new location or transitioning from a prolonged stationary state may require more frequent detection, while routine movement in known safe environments can minimize energy consumption.

The DULT Protocol must account for these power limitations in its design, ensuring that detection mechanisms remain effective without significantly degrading battery performance. Consideration of Device-specific constraints, such as variations in power efficiency across smartphones, wearables, and IoT devices, will be critical in maintaining a balance between security and usability.

4.2.3. Device constraints

Unwanted tracking detection is constrained by the diverse range of Devices used for scanning, each with varying hardware capabilities, operating system restrictions, processing power, and connectivity limitations. These factors directly impact the effectiveness of detection mechanisms and must be carefully considered in protocol design.

Hardware variability affects detection accuracy. While newer smartphones are equipped with advanced Bluetooth Low Energy (BLE) chipsets capable of frequent and reliable scanning, older smartphones, feature phones, and IoT devices may have reduced BLE performance. Differences in antenna sensitivity, chipset power, and OS-level access control can result in inconsistent detection, where some Devices fail to detect tracking signals as reliably as others.

Operating system restrictions can affect detection efforts, particularly due to background Bluetooth Low Energy (BLE) scanning policies. Both iOS and Android implement mechanisms to manage background scanning behavior, balancing energy efficiency and privacy considerations. On iOS, background BLE scanning operates with periodic constraints, which may limit the frequency of detection updates. Android applies similar policies to regulate background processes and optimize power consumption. Additionally, privacy frameworks on mobile Platforms may influence how applications access and process certain Accessory-related data. These factors, along with resource limitations in wearables and IoT Devices, can impact the feasibility of continuous scanning and detection.

Further, Platform permission models can restrict access to BLE scan data. For example, Android requires coarse or fine location permissions to perform BLE scanning, and users may revoke these permissions. Additionally, radio coexistence (BLE and Wi-Fi sharing the 2.4 GHz band) can impact BLE performance, especially on Devices with shared chipsets. User interface constraints, especially on wearables, may also limit how users receive or interact with tracking alerts.

Processing and memory constraints are another limiting factor, particularly for low-end mobile Devices and Tags. Continuous scanning and anomaly detection algorithms, especially those relying on machine learning-based threat detection, require substantial processing power and RAM. Devices with limited computational resources may struggle to maintain effective real-time detection without degrading overall performance. Ensuring that detection mechanisms remain lightweight and optimized for constrained environments is essential.

Connectivity limitations introduce additional challenges. Some Unwanted Tracking detection mechanisms rely on cloud-based lookups to verify Tag identities and share threat intelligence. However, users in offline environments, such as those in airplane mode, rural areas with limited connectivity, or secure facilities with network restrictions, may be unable to access these services. In such cases, detection must rely on local scanning and offline heuristics rather than real-time cloud-based verification.

To address these challenges, detection mechanisms should incorporate adaptive scanning strategies that adjust based on Device capabilities, optimizing performance while maintaining security. Lightweight detection methods, such as event-triggered scanning and passive Bluetooth listening, can improve efficiency on constrained Devices. Additionally, fallback mechanisms should be implemented to provide at least partial detection functionality even when full-featured scanning is not available. Ensuring that detection remains effective across diverse hardware and software environments is critical for broad user protection.

5. IANA Considerations

This document has no IANA actions.

6. Normative References

[I-D.detecting-unwanted-location-trackers]
Ledvina, B., Eddinger, Z., Detwiler, B., and S. P. Polatkan, "Detecting Unwanted Location Trackers", Work in Progress, Internet-Draft, draft-detecting-unwanted-location-trackers-01, 20 December 2023, <https://datatracker.ietf.org/doc/html/draft-detecting-unwanted-location-trackers-01>.

[I-D.draft-ietf-dult-Accessory-protocol]
"*** BROKEN REFERENCE ***".

[I-D.draft-ietf-dult-finding]
Fossaceca, C. and E. Rescorla, "Finding Tracking Tags", Work in Progress, Internet-Draft, draft-ietf-dult-finding-01, 6 June 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-dult-finding-01>.

[I-D.draft-ledvina-apple-google-unwanted-trackers]
Ledvina, B., Eddinger, Z., Detwiler, B., and S. P. Polatkan, "Detecting Unwanted Location Trackers", Work in Progress, Internet-Draft, draft-ledvina-apple-google-unwanted-trackers-01, 29 May 2025, <https://datatracker.ietf.org/doc/html/draft-ledvina-apple-google-unwanted-trackers-01>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

Acknowledgments

Many thanks for feedback from Brent Ledvina, Barry Leiba, Michael Ricardson, Eric Rescorla, Christine Fossaceca, Eva Galperin, and Alexis Hancock, and for contributed text from Corbin Streett and Diana Appanna. We also gratefully acknowledge the guidance and support of the DULT Working Group Chairs, Erica Olsen and Sean Turner, and the Area Director, Deb Cooley, throughout the development of this document.

Authors' Addresses

Maggie Delano
Swarthmore College
Email: mdelano1@swarthmore.edu

Jessie Lowell
National Network to End Domestic Violence
Email: jlowell@nnedv.org

Shailesh Prabhu
Nokia
Email: shailesh.prabhu@nokia.com