

Detecting Unwanted Location Trackers
Internet-Draft
Intended status: Informational
Expires: 7 February 2026

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

DULT Threat Model
draft-ietf-dult-threat-model-02

Abstract

Lightweight location tracking tags are in wide use to allow users to locate items. These tags function as a component of a crowdsourced tracking 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 location trackers 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 location tracking protocols, and provides design requirements, constraints, and considerations for implementation of protocols to detect unwanted location 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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 7 February 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	3
2. Conventions and Definitions	5
2.1. Conventions	5
2.2. Definitions	5
3. Security Considerations	6
3.1. Attacker access to victim account	6
3.2. Taxonomy of unwanted tracking	6
3.2.1. Example scenarios with analyses TODO: expand scenarios to incorporate expanded taxonomy	10
3.2.2. Bluetooth vs. other technologies	15
3.3. Possible Attacks on the DULT Protocol	15

3.3.1.	Threat Prioritization Framework for DULT Threat Model	15
3.3.2.	Threat Matrix	15
3.3.3.	Deploying Multiple Tags	18
3.3.4.	Remote Advertisement Monitoring	18
3.3.5.	Physically Modifying Tags	19
3.3.6.	Accessory Firmware Modifications	20
3.3.7.	Attacker Accessory Disablement	20
3.3.8.	Tracking Using Victim's Own Tag	20
3.3.9.	Disabling Victim Tag Detection	21
3.3.10.	Disabling Victim Tag	21
3.3.11.	Impersonation Attack (Tag)	22
3.3.12.	Impersonation Attack (Device)	23
3.3.13.	Replay Attack	24
3.3.14.	Heterogeneous Tracker Networks	24
3.4.	What is in scope	24
3.4.1.	Technologies	24
3.4.2.	Attacker Profiles	25
3.4.3.	Victim Profiles	25
3.5.	What is out of scope	25
3.5.1.	Technologies	25
3.5.2.	Victim Profiles	25
4.	Design Considerations	26
4.1.	Design Requirements	26
4.1.1.	Detecting Unwanted Location Tracking	26
4.1.2.	Finding Tracking Tags	30
4.1.3.	Disabling Tracking Tags	30
4.1.4.	Notification Management for Trusted Devices	31
4.1.5.	Privacy and Security Requirements (TODO)	32
4.2.	Design Constraints	32
4.2.1.	Bluetooth constraints	32
4.2.2.	Power constraints	33
4.2.3.	Device constraints	34
5.	IANA Considerations	35
6.	Normative References	35
	Acknowledgments	36
	Authors' Addresses	36

1. Introduction

Location tracking tags are devices that allow users to locate items. These tags function as a component of a crowdsourced tracking 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 an 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, reports its location to some central service.
- * The owner(s) queries the central service 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 tracking network, then the central server is able to track any accessory without the user's assistance, which is clearly undesirable.
- * Any attacker who can guess a tag ID can query the central server 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 tracking service with spoofed tag reports, disrupting real updates and overwhelming the central server.
- * Frequent co-location of multiple tags enables the central server or a passive observer to infer social relationships, routines, or group behaviors, compromising user privacy without consent.

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 tracker 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 location tracking could also occur in contexts where it is currently infeasible.

Detecting unwanted location tracking is currently left to individual tracking tag manufacturers and software on non-owner devices. Each manufacturer and smartphone operating system has different implementations to prevent unwanted location tracking, which may or may not be compatible with other manufacturers or operating systems. The goal of the IETF Detecting Unwanted Location Tracking (DULT) working group is to standardize a protocol between location tracking tags and non-owner devices.

In order to standardize a protocol for detecting unwanted location 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 location tracking, 2) methods attackers could use to circumvent unwanted location tracking protocols, and 3) design considerations for implementing unwanted location tracking protocols. The taxonomy of unwanted location tracking uses a flexible framework to provide analysis and modeling of different threat actors, as well as models of potential victims based on their threat context. It defines how these attacker and victim persona models can be combined into threat models. The section on methods to circumvent detection of unwanted location tracking 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 location tracking, alerting users, and providing guidance on disabling trackers (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].

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

- * ***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 device that is not easily discoverable and transmits location data to other devices.
- * ***easily discoverable***: a device 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 cm³ in three-dimensional space

3. Security Considerations

Incorporation of this threat analysis into the DULT protocol does not introduce any security risks not already inherent in the underlying Bluetooth tracking tag protocols. Existing attempts to prevent unwanted tracking by the owner(s) of a tag have been criticized as potentially making it easier to engage in unwanted tracking of the owner(s) of a tag. However, Beck et al. have demonstrated (<https://eprint.iacr.org/2023/1332.pdf>) a technological solution that employs secret sharing and error correction coding.

3.1. Attacker access to victim account

In a situation involving interpersonal control, an attacker may have access to a victim's tracking account (e.g. Apple FindMy). 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 victim'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 location trackers.

3.2. 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 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. 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 victim also has characteristics which influence the threat analysis. As with attacker characteristics, these are not intended as a definitive 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.
- * Expectation of unwanted tracking
 - Suspecting: The victim has reason to believe that unwanted tracking is a likely risk.
 - Unsuspecting: The victim has no particular reason to be concerned about unwanted tracking.
- * Access to resources
 - High: The victim 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 victim is generally unable to safely access practical and relevant resources. These might include money to pay a car mechanic or private investigator, law enforcement or legal assistance, or other 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.

It is also appropriate to define who is using the 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 victim's own tag to track them. Beck et al. describe a possible technological solution (<https://eprint.iacr.org/2023/1332.pdf>) to the problem of user privacy vs privacy of other potential victims. In designing the protocol, these concerns should be weighed equally. TODO: Is this actually how we want to weigh them? This warrants further discussion.

* Tracking tag usage

- 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.

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

* Tag placement

- Tag on victim's person or immediate belongings. This attack vector allows an attacker to track a victim 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 victim 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 victim. 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 location 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 victim from treating alerts seriously.

- Multiple tags using multiple types of placement. This attack vector may trick a victim 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 victim's precise location, monitoring a child's routine, monitoring car usage).

3.2.1. Example scenarios with analyses TODO: expand scenarios to incorporate expanded taxonomy

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 these 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 victim persona, or vice versa, to model a different scenario. For example, a non-expert victim persona could be combined with both non-expert and expert attacker personas.

3.2.1.1. Scenario 1

3.2.1.1.1. 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.

3.2.1.1.2. 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 victim.

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

Table 1

Victim Profile	Mango
Expertise Level	Non-Expert
Access to Resources	Low
Access to Technological Safeguards	Normal

Table 2

Other Characteristics	Avocado and Mango
Accessory Usage	Attacker Only

Table 3

3.2.1.2. Scenario 2

3.2.1.2.1. 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 tracker 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 their cannot take the car to the mechanic without Elderberry knowing.

3.2.1.2.2. Analysis

Here, the attacker and the victim are still cohabiting, and the attacker is monitoring the victim’s independent activities. This would allow the attacker to know if, for instance, the victim went to a police station or a domestic violence agency. The victim has reason to think that they are being tracked, but they cannot find the device. This can happen if the sound emitted by the device 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 victim 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 [I-D.detecting-unwanted-location-trackers]. In near-owner state it would not provide alerts under that specification.

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

Table 4

Victim Profile	Strawberry
Expertise Level	Non-Expert
Access to Resources	Low
Access to Technological Safeguards	Impaired (cannot hear alert sound)

Table 5

Other Characteristics	Elderberry and Strawberry
Accessory Usage	Attacker Only

Table 6

3.2.1.3. Scenario 3

3.2.1.3.1. 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 trackers, 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.

3.2.1.3.2. Analysis

This is a case involving a high-skill attacker, with a large skill difference between attacker and victim. 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 victim 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 victim to engage in active scanning, or to receive alerts on their phone. The victim 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 Victim	High
Access to Resources	High

Table 7

Victim Profile	Lime
Expertise Level	Non-Expert
Access to Resources	Low
Access to Technological Safeguards	Low

Table 8

Other Characteristics	Lemon and Lime
Accessory Usage	Attacker Only

Table 9

3.2.2. 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 crowd-sourced location tracking 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 crowd-sourced location tracking network.

3.3. 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 victim without their consent or otherwise take advantage of the crowdsourced network. These include deploying multiple tags to follow a single victim, 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.

3.3.1. 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 devices. To assess and prioritize these risks, the following framework classifies threats based on their impact, likelihood, feasibility, 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.

3.3.2. Threat Matrix

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

- * 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:
 - Victims: Individuals specifically targeted or affected by the attack.
 - 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	Impact	Likelihood	Risk Level	Affected Users	Mitigation Available?
Deploying Multiple Tags	Medium	High	High	Victims	Full
Remote	Medium	High	Medium	All	Partial

Advertisement Monitoring				users	
Physically Modifying Tags	High	Medium	Medium	Victims	Partial
Accessory Firmware Modifications	High	Low	Medium	Victims	Partial
Attacker Accessory Disablement	Medium	Medium	Medium	Victims	Partial
Tracking Using Victim's Own Tag	High	Medium	High	Victims	Partial
Disabling Victim Tag Detection	High	Medium	Medium	Victims	Partial
Disabling Victim Tag	Medium	Medium	Medium	Victims	Partial
Impersonation Attack (Tag)	High	Medium	High	Victims	Partial
Impersonation Attack (Device/Tag)	High	Medium	High	All users	Partial
Impersonation Attack (Device/Network)	Medium	Low	Low	All users	Partial
Replay Attack	Medium	High	Medium	Victims	Partial
Heterogeneous Tracker Networks	High	Medium	Medium	Victims	No

Table 10

3.3.3. Deploying Multiple Tags

When an attacker deploys tracking tags to follow a victim, 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 device is suspected of being used for unwanted tracking, and the time to do so must not be significantly impeded by the presence of multiple trackers. This also applies to situations where many tags are present, even if they are not being used for unwanted location tracking, such as a busy train station or airport where tag owners may or may not be in proximity to their tracking tags. Instead of distributing multiple tags in the same location, an attacker could also distribute multiple tracking tags across locations frequently visited by a victim (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 trackers, 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 3.3.6) or periodically disabling a tag (Section 3.3.7) to evade detection.

3.3.4. Remote Advertisement Monitoring

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 victim 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]). Beck 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 3.3.3).

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 device over time. Prior research, such as Beck 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 devices using rotating identifiers can be deanonymized through RSSI-based correlation techniques.

3.3.5. Physically Modifying Tags

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 trackers, leading to a high impact.

The likelihood is medium, as such hardware modifications require moderate technical expertise and physical access to the device. 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.

3.3.6. Accessory Firmware Modifications

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 device 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.

3.3.7. Attacker Accessory Disablement

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://undetecitag.com/products/undetecitag>).

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 victim'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 location tracking and maintaining the same identifier on reset.

3.3.8. Tracking Using Victim's Own Tag

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

This threat differs from impersonation or replay attacks (see Section 3.3.11 and Section 3.3.13) 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.

3.3.9. Disabling Victim Tag Detection

An attacker might intentionally disable passive unwanted location tracking detection on a victim's device. The impact of this attack is high as it would prevent the victim from being notified about possible unwanted location tracking.

The likelihood is medium, as executing this attack requires the attacker to physically or remotely alter settings on the victim's device, which involves moderate effort and access. The risk level is high. This attack can be partially mitigated by notifying victims of potential location tracking using other means e.g. sounds or haptics on location tracking tags.

3.3.10. Disabling Victim Tag

An attacker might intentionally disable a victim's tag as a form of harassment. This could be done with physical access to the tag, using a victim'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 victim'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.

3.3.11. Impersonation Attack (Tag)

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 device 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 crowdsourced location networks. 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 tracker identities and prevent these attacks. Operating systems can partially mitigate software impersonation attacks by restricting low-level BLE broadcasting unless elevated privileges are granted.

3.3.12. Impersonation Attack (Device)

In addition to impersonating a tag, an attacker could also impersonate a device. This affords attacks against both tracking accessories and against the crowdsourced network.

3.3.12.1. Attacks on accessories

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 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 location tracking and the accessory can confirm that a device has used other finding techniques to locate the device. (TODO remote disablement requirements section)

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.

3.3.12.2. Attacks on crowdsourced 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 no 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.

3.3.13. Replay Attack

In addition to impersonating legitimate tracking devices (see Section 3.3.11), attackers can record and replay Bluetooth advertisements from a legitimate tracker. For example, an attacker could capture a tracker'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 a tracker 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.

3.3.14. Heterogeneous Tracker Networks

Attackers may use a mix of tracking devices 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 tracker 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. What is in scope

3.4.1. Technologies

The scope of this threat analysis includes any accessory that is small and not easily discoverable and able to transmit its location to other consumer devices. Larger and/or easily discoverable devices such as laptops with tracking tag integrations may also choose to implement the protocol.

3.4.2. Attacker Profiles

An attacker who deploys any of the attacks described in Section 3.3.1 is considered in scope. This includes attempts to track a victim using a tracking tag and applications readily available for end-users (e.g. native tracking application) is in scope. Additionally, an attacker who physically modifies a tracking tag (e.g. to disable a speaker) is in scope. An attacker who makes non-nation-state level alterations to the firmware of an existing tracking tag or creates a custom device that leverages the crowdsourced tracking network is in scope.

3.4.3. Victim Profiles

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

3.5. What is out of scope

3.5.1. Technologies

There are many types of technology that can be used for location tracking. In many cases, the threat analysis would be similar, as the contexts in which potential attackers and victims exist and use the technology are similar. However, it would be infeasible to attempt to describe a threat analysis for each possible technology in this document. We have therefore limited its scope to location-tracking accessories that are small and not easily discoverable and able to transmit their locations to other devices. The following are out of scope for this document:

- * App-based technologies such as parental monitoring apps.
- * Other Internet of Things (IoT) devices.
- * Connected cars.
- * User accounts for cloud services or social media.

3.5.2. Victim Profiles

N/A

4. Design Considerations

As discussed in Section 3, unwanted location tracking can involve a variety of attacker, victim, and tracking tag profiles. A successful implementation to preventing unwanted location 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 3.4 and Section 3.5
- * Account for scenarios in which the victim has low expertise, access to resources, and/or access to technological safeguards within the scope defined in Section 3.4 and Section 3.5
- * Avoid privacy compromises for the tag owner(s) when protecting against unwanted location tracking using tracking tags

4.1. Design Requirements

The DULT protocol should 1) allow victims to detect unwanted location tracking, 2) help victims 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 victims to disable those trackers 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 victims in detecting potentially unwanted location 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 victim 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 tracking tags that are separated from their owners. 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 4.1.5). 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

The platform should passively scan for devices suspected of unwanted location tracking and notify the user. This will involve implementing one or more algorithms to use to flag trackers 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 location tracking, the user should be able to view the serial number of the device along with obfuscated owner information (e.g. last four digits of phone number, obfuscated email address) 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 location tracking promptly and alerting the potential victim 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 tracking devices, 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 location tracking. Each factor can be considered independently to help inform an overall risk assessment.

4.1.1.2.1. Duration of Proximity

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

Rationale: Devices 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).

4.1.1.2.1.1. Movement Correlation

Measures how closely the movement of the suspected device 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 device is following the user intentionally.

4.1.1.2.1.2. Signal Strength Trends

Observes how the signal strength of the suspected device (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.

4.1.1.2.1.3. Persistence

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

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

4.1.1.2.1.4. Hardware Identity

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

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

4.1.1.2.1.5. Environmental Context

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

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

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 devices. Instead of triggering alerts based solely on presence, the system can dynamically adjust its sensitivity based on behavioral patterns. For example, if a tracking device

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 tracker 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 tracker 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 tracker was briefly detected nearby.")
 - Medium confidence: Warning with recommended actions (e.g., "A tracker has been detected multiple times near you. Check your surroundings.")
 - High confidence: Urgent alert with mitigation options (e.g., "A tracker 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.

4.1.1.3. Tracking Tag Alerts

Tracking tags may be difficult to locate, and users may not have a device that can actively or passively scan for 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, 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.

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 location tracking.

Logs should include sufficient detail to detect unwanted location tracking without being another vector for surveillance. For example, a log could state that "User B viewed the location of device X at [time]." By including information about user, device, 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 location tracker 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 tracker through passive or active scanning to request that the tracker 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. Platforms may also implement other methods to assist in locating trackers, such as precision finding using Ultra-wideband.

4.1.3. Disabling Tracking Tags

In order to effectively prevent unwanted location tracking, users should be able to disable location tracker 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 tracking tags once they are located.

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 tracker 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 device 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 tracker, even if the tag is not from the same platform. Serial numbers may be used to report the device, 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 trackers 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 Devices

To reduce alert fatigue and improve user experience, implementations should allow users to snooze passive notifications from 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 trackers. Platforms should make it easy to manage snoozed devices 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 tracker. However, this introduces the risk of abuse (e.g., an attacker adding a victim 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 location tracking (see Section 4.1.1.2).

4.1.5. Privacy and Security Requirements (TODO)

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 trackers requires analyzing Bluetooth Low Energy (BLE) advertisement packets. Most advertisements are publicly transmitted, allowing passive scanning by any nearby receiver. While this enables open detection of unknown tracking devices, 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 location tracking 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 tracking devices. 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 tracking device 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. Additionally, passive Bluetooth listening techniques could serve as a low-power alternative to active scanning, allowing background detection without excessive battery drain.

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 device-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 embedded systems. 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 tracker 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]

Ledvina, B., Lazarov, D., Detwiler, B., and S. P. Polatkan, "Detecting Unwanted Location Trackers Accessory Protocol", Work in Progress, Internet-Draft, draft-ietf-

dult-accessory-protocol-00, 3 November 2024,
<<https://datatracker.ietf.org/doc/html/draft-ietf-dult-accessory-protocol-00>>.

[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>>.

[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

TODO acknowledge.

Authors' Addresses

Maggie Delano
Swarthmore College
Email: mdelanol@swarthmore.edu

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

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