# DULT Threat Model v03 Overview

Maggie Delano, Swarthmore College

# Agenda

1. Threat model (w/ Threat model co-authors)
    a. Motivation
    b. New in v03
    c. Open issues
2. Remote disablement (w/ Accessory Protocol authors)
    a. Goals
    b. Implementation
    c. Questions

# Motivation

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

- DULT Threat Model has been adopted by the WG and includes:
  - A taxonomy of unwanted tracking
  - Methods to Circumvent DULT Protocol (attacks)
  - Design requirements and constraints

# New in v03

- Major changes
  - Adds additional scenarios to taxonomy
  - Adds recommendations regarding GPS trackers
  - Overhauls terminology (updated terminology at the top, updates text to reflect new terminology)

# Open issues

- Major changes
  - **Consider moving attacks before taxonomy**
- Clarifications/ minor improvements
  - Add entry for Tag
  - Move requirement out of definitions
  - Change capitalization in intro/abstract
  - "Unwanted Tracking Alert" definition is unclear (open w/ PR)
  - Clarify security risks with threat model
  - Consider renaming section 3.1 Security Considerations Unique To Unwanted Location Tracking
  - Consider renaming Security Considerations section
  - Consider differences between technically sophisticated attacks that can be packaged up versus ones that require physical manipulation

https://github.com/ietf-wg-dult/threat-model/issues

# Consider moving attacks before taxonomy #160

Watson Ladd wrote:

*IMHO, I think we should start by describing what Attackers can do. They can place tags on Victims or their belongings, they can try to exploit existing tags the Victim has either secretly or by attempting to trigger them, etc. That's material we have in 3.4, and I think a lot of it isn't circumventing DULT, but rather general attacks. Then we can have the taxonomy of various attack scenarios. It is not easy reading, and I know it was not easy to write. I think it very much belongs in this document: the stakes are real.*

*Once we have that down, then the motivation and background to understand the concerns about tags needing to be easy to locate even after notification, in a multimodal way, or need for devices implementing to be able to work stand-alone, are present. This would be the material in 3 that's dult specific or in depth responses to particular aspects of the attacks in the taxonomy. My hope is that this reorganization makes it easier to find what mitigations are required where when searching in the doc and makes it easier to read through and understand. Conceptually we have threat model, taxonomy of attacks, and then mitigations for things the DULT protocol itself cannot in this new organization.*

(MD note: I'm definitely open to this but I think we can probably make the smaller changes first and see where that leaves us.)

# Current Table of Contents

# Other feedback on the threat model doc?

# Remote Disablement (Accessory Protocol

# Goal of remote disablement

- There might be situations where the tracker is very well hidden and cannot be physically located by the target. In this scenario, despite receiving multiple alerts on their phone, the target cannot locate the tag and disable it.
- This presentation discusses proposed implementation of the feature.

# Disabling Tags

- A tag may be disabled (i.e. its location will no longer be crowdsourced) if all of the following conditions are met:
  - A tag is away from its owner
  - A user has successfully triggered the “play sound” command at least 5 times
  - The tag has been in range to the device seeking to disable the tag for at least 10 minutes
- To disable a tag, an op code is sent to the tag using the non-owner device protocol
- When a tag has been disabled, the tag continues to advertise but sets a specific bit that indicates it is disabled and its location should not be used for crowdsourcing.

# Disabling tags (cont.)

- When a tag has been disabled, it can be re-enabled under any of the following conditions:
  - The tag owner has connected to the tag / returned into range
  - When the tag has been power cycled
  - When directed by the crowdsourced network (e.g. valid court order)
- When a tag is re-enabled, the user who disabled the tag is notified, along with the last known location of the tag

# Proposed Technical Implementation

- A tag is away from its owner
  - Already established in accessory-protocol
- A user has successfully triggered the “play sound” command at least 5 times
  - Tag can count number of “play sound” commands received in a given time period
- The tag has been in range to the device seeking to disable the tag for at least 10 minutes
  - Implement new Opcode for remote disablement command. The tag only disables after receiving the command once per minute for 10 minutes.
  - (Would require some implementation to ensure the commands are coming from the same device; suggestions welcome on how to do that)

# Security Considerations

- A non-conformant device could transmit a remote disablement command without abiding by the requirements. Requirements must be enforceable by the tag to mitigate the impact of this attack:
  - A tag is away from its owner
  - A user has successfully triggered the “play sound” command at least 5 times
  - The tag has been in range to the device seeking to disable the tag for at least 10 minutes

# Security Considerations (cont.)

- There may be scenarios where an attacker attempts to remotely disable a tag in a scenario other than the target scenario (e.g. on the bus or at an airport). The remote disablement requirements should be sufficiently onerous to deter mass disablement.
  - Tags that are near owners cannot be remotely disabled.
  - If a tag is disabled, legitimate owners can enter Bluetooth range and/or power cycle a tag to re-enable it.
  - The “play sound” (or haptic equivalent) should alert those nearby that someone is attempting to disable a tag, but they will not be able to stop a tag from being disabled.
- Remote disablement is added redundancy. If an attacker already has physical possession of a tag, they can disable it manually anyway. Attackers can already use the “play sound” feature today. The only addition is remote disablement.

# Considered but not recommended

- It would be ideal to restrict remote disablement commands to tags that are suspected of unwanted location tracking. This would require knowledge that cannot be enforced by the tag:
  - Knowledge that an unwanted tracking alert has triggered (only known via device)
  - Knowledge that a tag is moving with a device (only available by proxy in some tags with accelerometers, and would require implementation that may be infeasible for some tags)
- Therefore our proposal does not require either of these conditions

# Considered but not recommended (cont.)

- A “snooze” feature to temporarily remotely disable, instead of a non-timed disablement
  - The current proposal states that remote disablement should only be reversible by non-timed conditions (e.g. tag owner in range). This is because only allowing targets to “snooze” tags would require disabling the tag at regular intervals, which could cause undue stress.
  - One possibility is to allow for non-timed and timed remote disablement, but this added complexity does not add much.
- Allowing a user to opt their device out of the crowdsourced network only
  - May provide a false sense of security and does not mediate ability of network to track the target in sufficiently well-populated areas (though its effectiveness would be higher in lower density areas)

# Questions

- What are the costs of tags being disabled remotely over the air?
  - Is it okay if attackers are able to mass disable tags?
  - Is there a meaningful downside besides anti-theft, which we are not considering for the WG?
- How do we make it hard enough to dissuade attackers, but still helpful for targets? (is 10 mins reasonable?)
- Do we have sufficient enforceability by tags?