

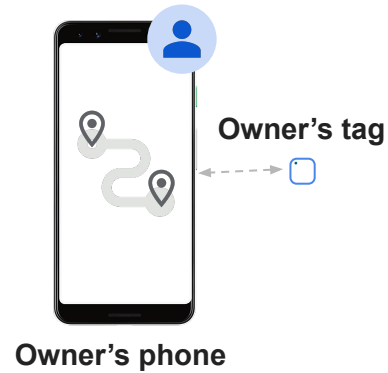
# Detecting Unwanted Location Trackers

BoF Presentation  
July 27, 2023

# System Architecture

(How Bluetooth Crowdsourcing and Unwanted-Tracking Detection Work)

# Near-owner mode



## Near-owner mode

- Phone physically close to accessory
- Persistent or periodic BT connection keeps accessory in near-owner mode

# Separated mode

Owner's tag

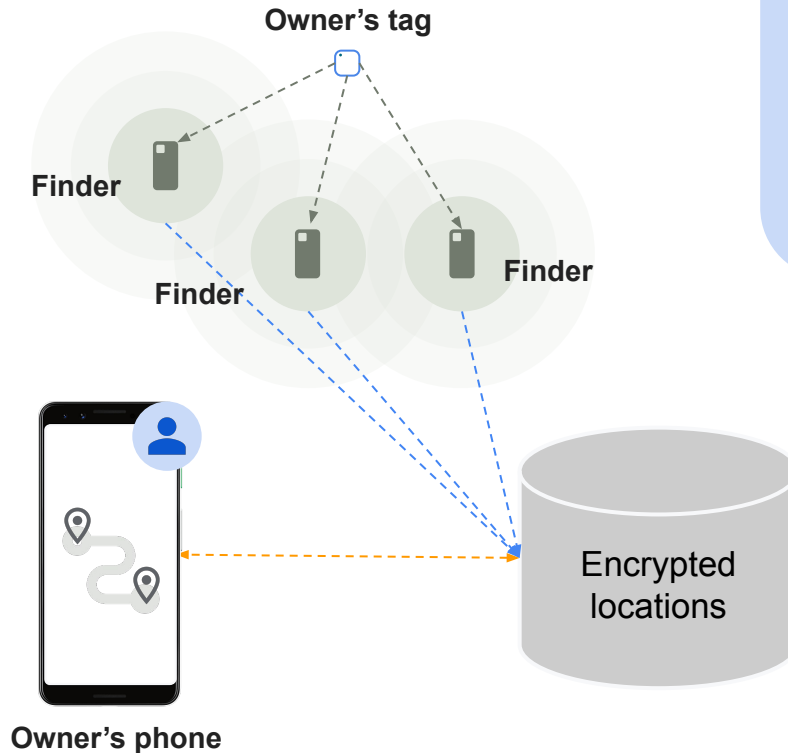


Owner's phone

## Separated Mode

- Phone physically far away
- OR could be powered off or have dead battery

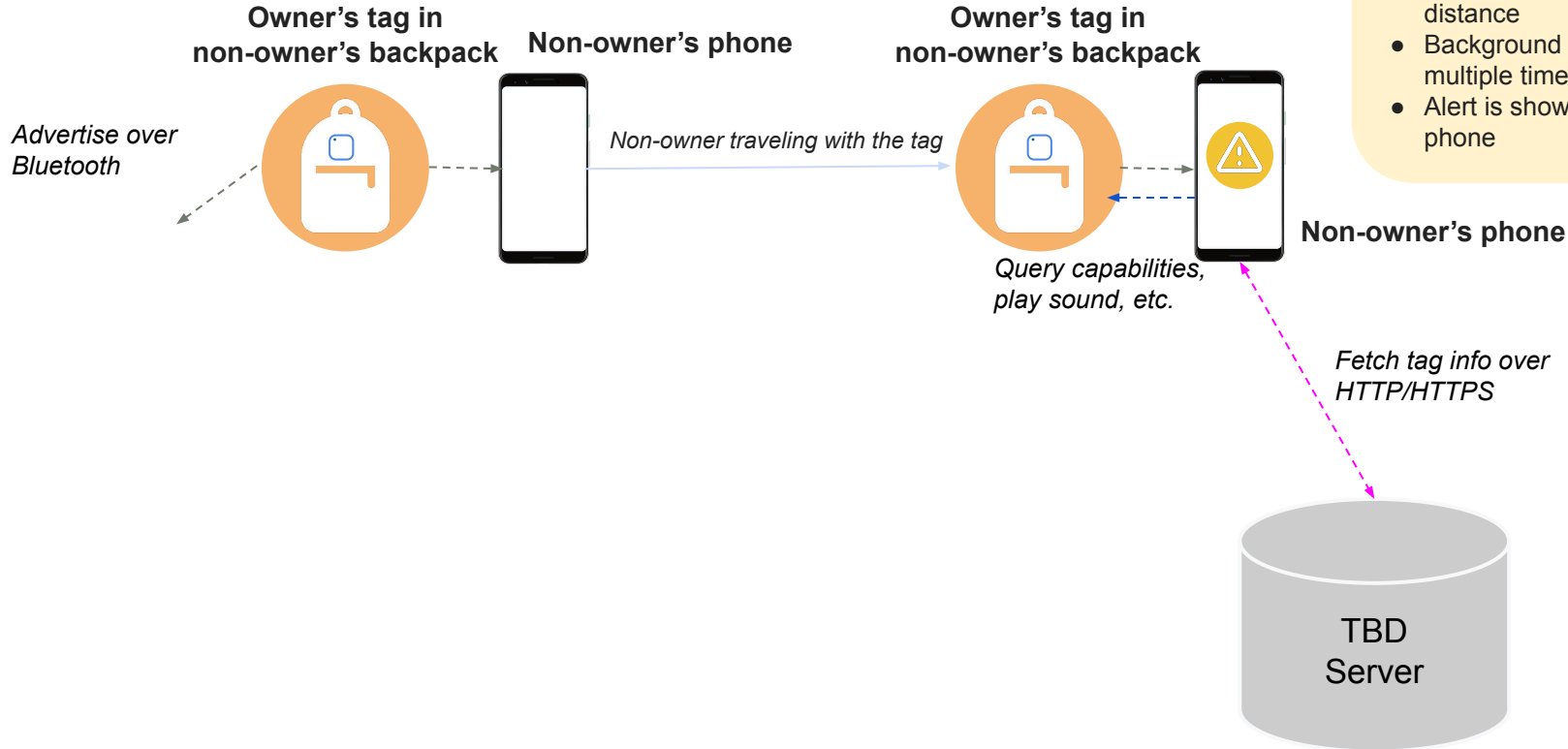
# Separated mode + Bluetooth (BT) crowdsourcing



## Crowdsourcing

- Finders observe BT advertisement
- Finders encrypt their own location using key in advertisement
- Finders upload encrypted locations to server
- Owner's phone queries locations from the server, decrypts them, and computes best-estimate of location

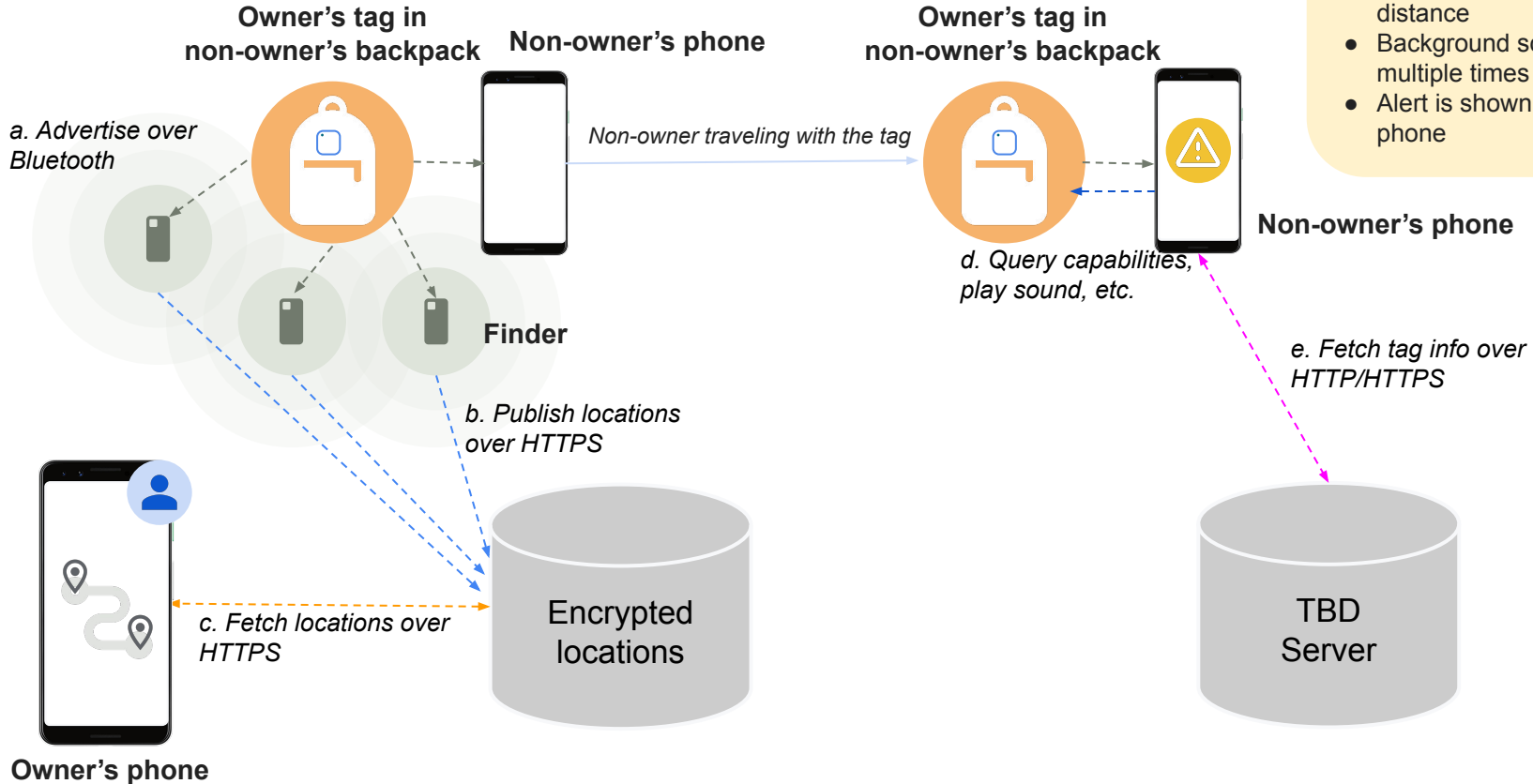
# Architecture: Unwanted tracking



## UT detection and alerting

- Tag is separated from owner
- Tag has been moving with non-owner over time and distance
- Background scans detect tag multiple times
- Alert is shown on non-owner's phone

# Architecture: BT crowdsourcing + unwanted tracking



## UT detection and alerting

- Tag is separated from owner
- Tag has been moving with non-owner over time and distance
- Background scans detect tag multiple times
- Alert is shown on non-owner's phone

# Comparison of some existing systems

Surface	Deterrence at pairing	Proactive alerts (background scanning)	Learn about accessory	Non-owner play sound	Serial number look-up	Accessories detected
iOS UT	✓	✓	✓	✓	✓	AirTags + AirPods + Apple FMN accessories
Android UT	N/A	✓	✓	✓	✓	AirTags + Google FMD accessories
Airguard app	N/A	Android: yes iOS: Tile + Samsung tags	✗	✓	✗	All accessories?
Tile app	Under consideration	Under consideration	✓	Under consideration	✓	Tile tags and Tile partner's accessories

# Threat Model

Persona	Threat	Proposed Mitigations
Stalker	Uses location-enabled accessory for unwanted tracking	Enable target to find and trace accessory (below)
Target	Target unaware of unwanted tracking	24 hour BT address stability
	Target unable to find tracking accessory	Play sound on item
		Alternate finding hardware
	Target didn't receive alert soon enough	Scan for items
	Target unable to receive unwanted tracking alert	Beep on Move
	Target unable to identify known stalker	Obfuscated Owner Information
	Target or Other working on Target's behalf unable to trace stalker	Serial no. visible
		Serial no. over NFC/BT
Pairing Registry		
Target unable to disable location share	Can disable finding	
Third-Party Scanner	Owner tracked across physical space with BT address	BT MAC randomization + 30 min address rotation
	Target tracked across physical space with BT address	BT MAC randomization + 24 hour address rotation
	Owner tracked across physical space with serial no. broadcast	Action required for broadcast + encryption
Accessory Hacker	Firmware overwritten to eliminate unwanted tracking protections	-
Non-Adherent Manufacturers	Accessory manufacturers implement spec incorrectly, incompletely, or not at all	-

# Scope

# Architecture: BT crowdsourcing + unwanted tracking

Partially in scope

a. Advertise over Bluetooth

Owner's tag in non-owner's backpack  
Non-owner's phone

Non-owner traveling with the tag

Owner's tag in non-owner's backpack

d. Query capabilities, play sound, etc.

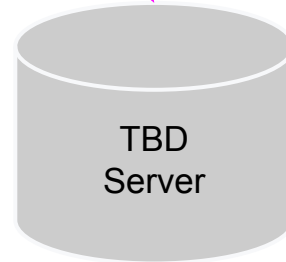
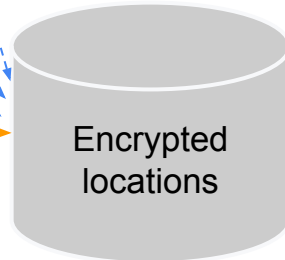
In scope

Non-owner's phone

In scope

e. Fetch tag info over HTTP/HTTPS

b. Publish locations over HTTPS



c. Fetch locations over HTTPS



## UT detection and alerting

- Tag is separated from owner
- Tag has been moving with non-owner over time and distance
- Background scans detect tag multiple times
- Alert is shown on non-owner's phone

# Scope of Charter Proposal – Goals

The goal of the DULT WG is to standardize a protocol for information exchange between location-tracking accessories and nearby devices, along with actions that these accessories and devices should take once unwanted tracking is detected. The intent of this WG is to make it easier for arbitrary devices to detect unwanted tracking by these accessories. The protocols and interactions between devices may be limited to certain states or modes, such as the accessory being separated from a paired/owner device.

The privacy goals of the WG solution are that:

- The owner of the tracking accessory must not learn information about nearby devices that discover or interact with the tracking accessory
- The interactions between tracking accessories and nearby devices are secure
- Actions available to a nearby device (e.g., playing a sound on a tracking accessory) can be limited to certain states or modes

The WG protocol design will be guided by an intent to:

- Minimize hardware changes needed in tracking accessories to implement this protocol; and
- Not preclude adoption by manufacturers of larger devices whose primary purpose is not location tracking, but have location tracking capabilities (e.g., headphones, bicycle, smartphone)

# Scope of Charter Proposal – Program of Work

The WG is expected to:

1. Standardize a protocol between tracking accessories and nearby devices, which may:
  - Allow a tracking accessory to identify & advertise its presence when in a detectable mode
  - Allow a nearby device to trigger behavior on an unwanted tracking accessory to aid in determining its physical location
  - Allow nearby devices to fetch additional information about a tracker accessory
2. Specify practices that accessory manufacturers can implement to deter malicious use of tracking accessories and support the implementation of the WG-specified protocol.
3. Specify guidance for non-owner device platforms necessary to support implementation of the WG specified protocol

# Not in Scope for This Spec

The WG will **not** standardize an end-to-end platform-based unwanted tracking detection system or define requirements for interactions between accessory manufacturers and law enforcement. In addition, these items are out-of-scope:

- Mechanisms for detecting tracking accessories that do not implement the protocol specified by the WG, and
- Mechanisms for detecting whether a tracking accessory implements the protocol or allowing a tracking accessory to attest that it implements the protocol

# Apple Licensing Commitment

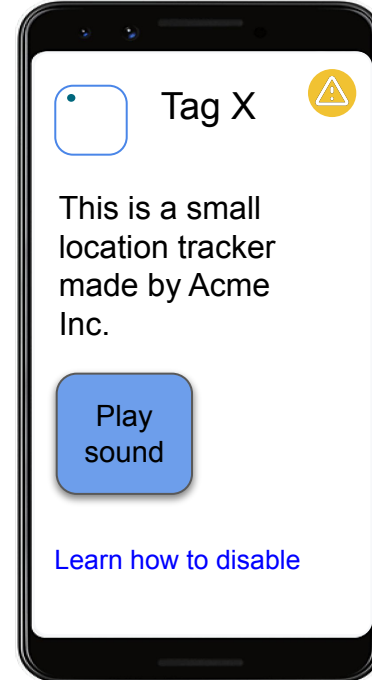
- Apple has timely submitted IPR disclosures under the rules of the IETF IPR Policy, RFC 8179, committing to license under RAND terms, for the purpose of implementing the Detecting Unwanted Location Trackers specification, any patent claims that would necessarily be infringed by implementation of such specification.
- Apple has made similar RAND commitments over the years and has publicized its commitment to RAND licensing principles to advance interoperability and give consumers confidence that products will interact reliably with each other.

Questions?

# Back-up

# Proactive Alert

- Proactive alert shows
  - Tag image
  - Text description
  - Play sound button
  - Disablement text instructions (potentially including diagram/video)
  - Etc.



# Proposed BT advertisement header in Internet Draft

Bytes	Description	Requirement
0-5	MAC address	REQUIRED
6-8	Flags TLV; length = 1 byte, type = 1 byte, value = 1 byte	OPTIONAL
9-12	Service data TLV; length = 1 byte, type = 1 byte, value = 2 bytes (TBD value)	REQUIRED
13	Protocol ID (TBD value)	REQUIRED
14	Near-owner bit (1 bit) + reserved (7 bits)	REQUIRED
15-36	Proprietary company payload data	OPTIONAL

More discussion needs to be had on how to best limit privacy-violating uses of the proprietary data. Proposal: analysis and discussion of this part should be in scope of charter