Systematizing the Offline Finding Landscape

Over the last decade, a revolution in location-tracking technology has changed how we keep track of our belongings. Known as **Offline Finding (OF)** systems, these networks enable users to locate a device even when it's not connected to the internet or anywhere near them.

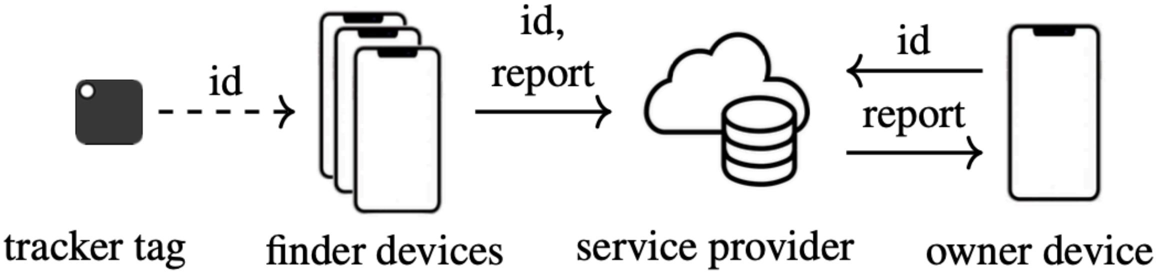


Figure 1: A summary of the interactions in an OF protocol.

The idea is simple: billions of participating internet-connected "finder" devices—phones, tablets, and laptops—listen for advertisements from low-cost, Bluetooth-only tracker tags. If one of these finders detects a short-range Bluetooth signal from a lost tracker, it forwards that information to the vendor's servers, along with its own location. The owner of the tag can then query the vendor to see where their tag was last spotted. We summarize these interactions in Figure 1.

The opaque world of OF protocols

Tile popularized OF systems via its protocol and proprietary tags in 2014. Today, Apple (Find My), Google (Find My Device), Samsung (SmartThings Find), and Life360 (Tile) operate massive networks covering billions of devices. What began as a handy way to recover lost items has grown into a global, always-on location-tracking infrastructure.

Despite their scale, these systems are remarkably opaque. Vendors keep their designs proprietary and offer minimal documentation. Academic researchers have had to reverse engineer their protocols piece by piece to understand how they work [1, 2, 3, 4]. As a consequence, there has been no comprehensive, cross-vendor security and privacy analysis.

This lack of transparency is consequential because the same features that make OF networks great for finding lost keys also make them ripe for abuse. Indeed, a tracker built to locate a bag can just as easily be hidden in someone's car to follow their movements.

Early OF deployments appeared to overlook this threat, perhaps because they assumed network participants were benign. That assumption collapsed as real-world abuse-cases emerged—stalking, theft, physical assault, and even murder [5, 6, 7]—linked to AirTags, Tiles, and similar devices.

An assortment of “Anti-Stalking” fixes

Under public pressure, vendors rushed to add “anti-stalking” features. These typically alert users when an unknown tracker has been moving with them for an extended period. But there’s no industry standard: each vendor’s approach is different, often incompatible with others, and varies widely in effectiveness.

The result is a fragmented abuse-detection system. A stalker could simply choose a tracker from a vendor whose alerts are less effective or one that isn’t integrated with the victim’s phone.

Balancing privacy and abuse prevention

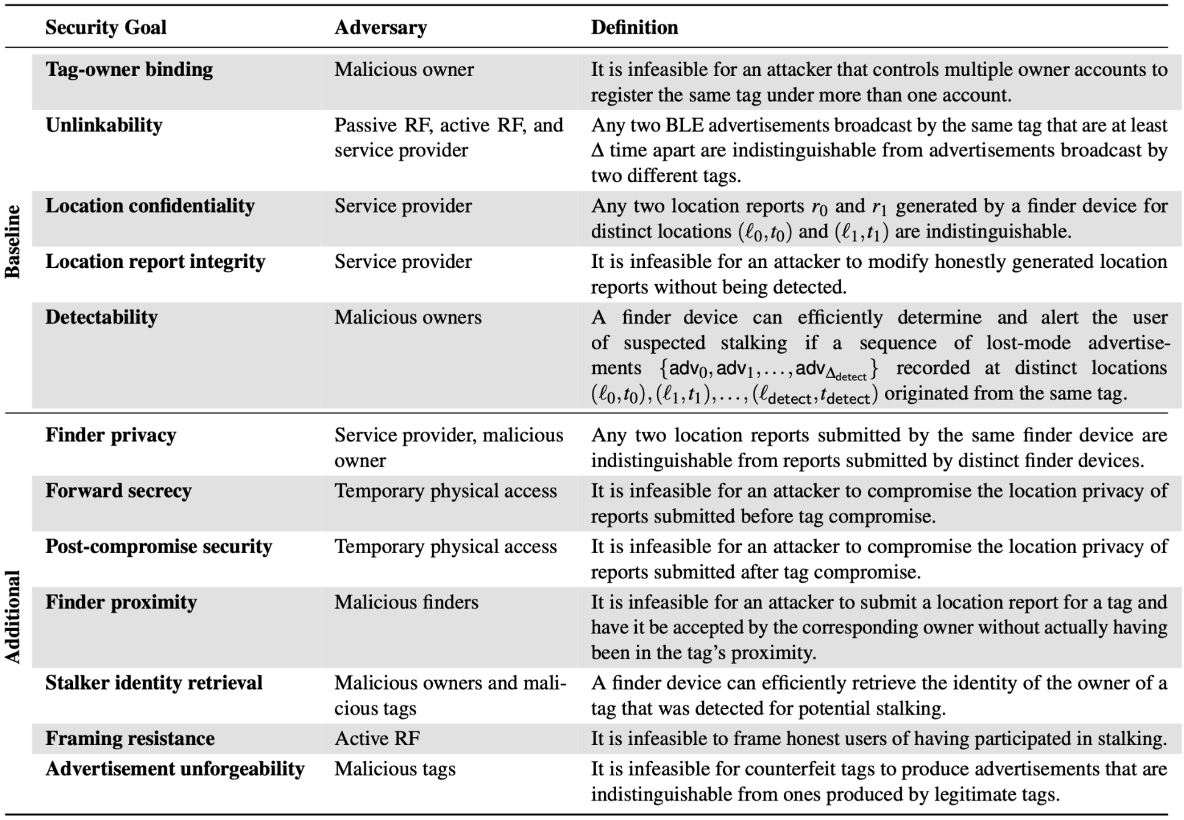
The complexity of building and analyzing these systems is exacerbated by their inherently conflicting privacy and abuse-prevention goals. On the one hand, privacy requires that a tag’s Bluetooth advertisements be frequently rotated and *unlinkable*, so that no one can fingerprint the tag and track its owner over time. On the other hand, abuse-prevention requires the opposite: finder devices must be able to *link* a tag’s advertisements in order to detect when a rogue tag is following them. Cryptography helps reconcile these goals, but every vendor solves the problem differently, and the details are rarely public. Without transparency, it’s hard for researchers or policymakers to assess whether the solutions are secure or even functional.

Our work

We are the first to systematize the security and privacy landscape of OF protocols across vendors. For this, we reviewed over fifty academic papers that analyze various properties of OF protocols, and categorized them into six categories: (1) Security analysis of OF protocols, (2) Security definitions and secure construction proposal, (3) Antistalking feature analysis/proposal of antistalking tools, (4) Security analysis of Bluetooth Low Energy communications with focus on OF protocols, (5) Abusability of OF protocols, (6) OF usability, and (7) Proposals for/analysis of OF-inspired crowdsrouced networks.

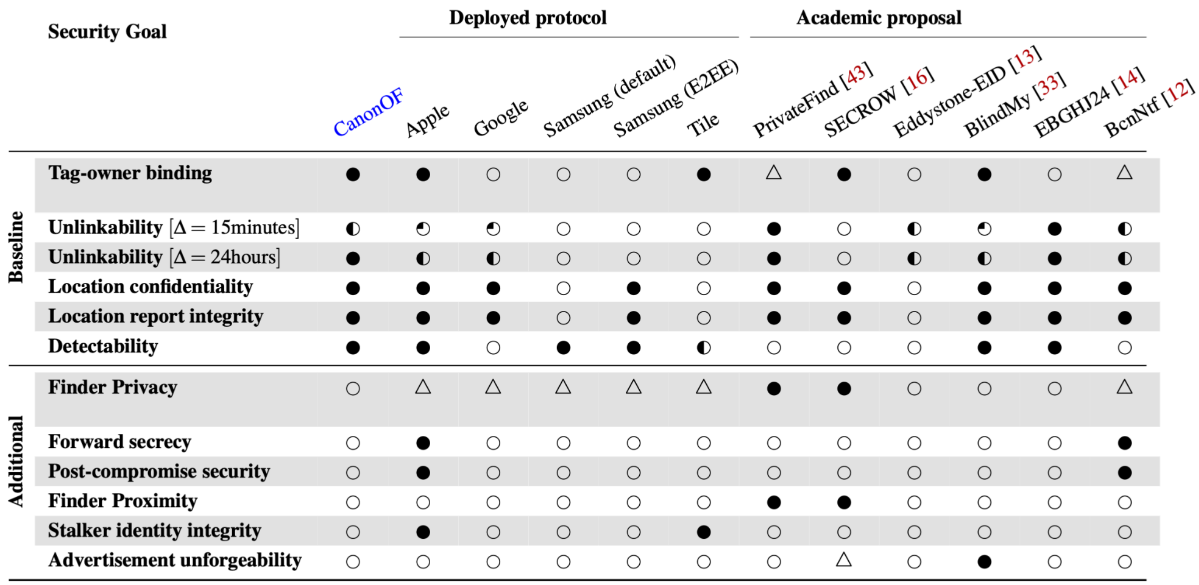
Additionally, we reviewed vendor specifications for Apple, Google, Samsung, and Tile, as well as the IETF draft for standardizing OF protocols, which we categorized as Industry specification/IETF draft.

We then combined this prior research with our own experiments to reconstruct how Apple, Google, Samsung, and Tile implement their OF protocols. To evaluate these designs, we built a security framework based on known vulnerabilities, formal security definitions from academic work, as well as our own definitions (summarized in Table 1). This allowed us to assess each system against a consistent set of goals. Along the way, we gave a simple OF construction, CanonOF, that achieves most of the security goals and which, we believe, serves as a canonical reference protocol that helps clarify essential design components underlying OF protocols. We summarize our results in Table 2.



	Security Goal	Adversary	Definition
Baseline	Tag-owner binding	Malicious owner	It is infeasible for an attacker that controls multiple owner accounts to register the same tag under more than one account.
	Unlinkability	Passive RF, active RF, and service provider	Any two BLE advertisements broadcast by the same tag that are at least Δ time apart are indistinguishable from advertisements broadcast by two different tags.
	Location confidentiality	Service provider	Any two location reports r_0 and r_1 generated by a finder device for distinct locations (ℓ_0, t_0) and (ℓ_1, t_1) are indistinguishable.
	Location report integrity	Service provider	It is infeasible for an attacker to modify honestly generated location reports without being detected.
	Detectability	Malicious owners	A finder device can efficiently determine and alert the user of suspected stalking if a sequence of lost-mode advertisements $\{\mathsf{adv}_0, \mathsf{adv}_1, \ldots, \mathsf{adv}_{\Delta_{\mathsf{detect}}}\}$ recorded at distinct locations $(\ell_0, t_0), (\ell_1, t_1), \ldots, (\ell_{\mathsf{detect}}, t_{\mathsf{detect}})$ originated from the same tag.
Additional	Finder privacy	Service provider, malicious owner	Any two location reports submitted by the same finder device are indistinguishable from reports submitted by distinct finder devices.
	Forward secrecy	Temporary physical access	It is infeasible for an attacker to compromise the location privacy of reports submitted before tag compromise.
	Post-compromise security	Temporary physical access	It is infeasible for an attacker to compromise the location privacy of reports submitted after tag compromise.
	Finder proximity	Malicious finders	It is infeasible for an attacker to submit a location report for a tag and have it be accepted by the corresponding owner without actually having been in the tag's proximity.
	Stalker identity retrieval	Malicious owners and malicious tags	A finder device can efficiently retrieve the identity of the owner of a tag that was detected for potential stalking.
	Framing resistance	Active RF	It is infeasible to frame honest users of having participated in stalking.
	Advertisement unforgeability	Malicious tags	It is infeasible for counterfeit tags to produce advertisements that are indistinguishable from ones produced by legitimate tags.

Table 1: Security goals for Offline Finding protocols and the corresponding threat model.



	Security Goal	Deployed protocol						Academic proposal					
		CanonOF	Apple	Google	Samsung (default)	Samsung (E2EE)	Tile	PrivateFind [43]	SECROW [16]	Eddystone-EID [13]	BlindMy [33]	EBGHJ24 [14]	BcnNtf [12]
Baseline	Tag-owner binding	●	●	○	○	○	●	△	●	○	●	○	△
	Unlinkability [$\Delta = 15\text{minutes}$]	◐	◔	◔	○	○	○	●	○	◐	◔	●	◐
	Unlinkability [$\Delta = 24\text{hours}$]	●	◐	◐	○	○	○	●	○	◐	◐	●	◐
	Location confidentiality	●	●	●	○	●	○	●	●	○	●	●	●
	Location report integrity	●	●	●	○	●	○	●	●	○	●	●	●
	Detectability	●	●	○	●	●	◐	○	○	○	●	●	○
Additional	Finder Privacy	○	△	△	△	△	△	●	●	○	○	○	△
	Forward secrecy	○	●	○	○	○	○	○	○	○	○	○	●
	Post-compromise security	○	●	○	○	○	○	○	○	○	○	○	●
	Finder Proximity	○	○	○	○	○	○	●	●	○	○	○	○
	Stalker identity integrity	○	●	○	○	○	●	○	○	○	○	○	○
	Advertisement unforgeability	○	○	○	○	○	○	○	△	○	●	○	○

Table 1: Summary of implementations and their achieved security properties. We use ● to denote that a protocol achieves a property, ◐ and ◔ to denote that a property is partially

achieved (i.e., only against certain adversaries or in specific modes of operation), and ○ to indicate that a property is not achieved. We use △ to indicate that it is unclear whether a protocol achieves a given property either because it needs more analysis of the protocol or because the protocol is underspecified.

Whenever a system failed to meet a goal, we traced the cause to a specific design choice or vulnerability and proposed mitigations. Some failures were due to intentional trade-offs (e.g., stronger stalking detection by compromising some privacy), while others were implementation flaws. We conclude by discussing major challenges in securing OF systems and outlining open research problems.

Why This Matters

The sheer scale of OF networks means they now form a global infrastructure, whether we like it or not. These systems can be used for good, but without careful design, they can also become tools for covert human tracking.

The stakes aren't just technical. There are deeper policy and societal questions: S*hould there be a global anti-stalking standard? How should law enforcement be involved? How can abusers of these systems be held accountable? And how do we reconcile the tension between making these systems useful and preventing their abuse?*

Our hope is that by clarifying how these systems work, where they succeed, and where they fail, we can guide both technical improvements and policy debates toward safer, more privacy-friendly designs.

Next Steps

We plan to submit our work to a top security conference this fall. Building on this foundation, we will pursue one of the key open challenges our study identified: incorporating accountability into OF systems. Accountability mechanisms enable potential victims to collaborate with platforms or external authorities to deter misuse by identifying and punishing malicious actors. Achieving this requires cryptographically binding tracker owners' identities to the protocol flow, so that in cases of abuse, authorized parties can reliably uncover the perpetrator's identity. Moving forward, we will work on defining formal cryptographic notions of accountability and exploring practical constructions that achieve them.

References

1. Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System

2. Privacy Analysis of Samsung's Crowd-Sourced Bluetooth Location Tracking System

3. A thorough security analysis of ble proximity tracking protocols

4. Okay google, where’s my tracker? security, privacy, and performance evaluation of google’s find my device network

5. https://www.washingtonpost.com/nation/2022/06/11/apple-airtag-murder-boyfriend-indianapolis-morris/

6. https://www.macrumors.com/2021/12/31/airtag-increasingly-linked-to-crime/

7. https://www.vice.com/en/article/y3vj3y/apple-airtags-police-reports-stalking-harassment