Surveilling the Masses with Wi-Fi-Based Positioning Systems

Leandro Costa, up202408816[1,✉]

[*]Surveilling the Masses with Wi-Fi-Based Positioning Systems, Erik Rye, Dave Levin, University of Maryland

Wi-Fi Positioning System | BSSID Tracking | Mass Surveillance

Introduction

The paper by Rye and Levin offers a compelling and concerning examination of the ways in which Apple's Wi-Fi-Based Positioning System (WPS) can be misused for mass surveillance. Originally designed to assist mobile devices in determining their geolocation more efficiently than GPS, WPS has inadvertently created a new avenue for significant privacy violations on a global scale.

The main issue arises from the way Apple's WPS functions: it responds to unauthenticated queries with geolocation data for any recognized Wi-Fi access point, identified by its MAC address or BSSID. Even more troubling, it does not just provide the location of the requested BSSID; it also returns the locations of hundreds of nearby BSSIDs, effectively multiplying the potential surveillance data exponentially.

Problem Description

Apple's WPS allows devices to query the location of nearby Wi-Fi access points (BSSIDs). These BSSIDs are unique identifiers tied to network hardware. Once collected through crowdsourcing, this data is used to estimate a device's location. However, Apple's API is publicly accessible, unauthenticated, and highly permissive: it responds to queries from any device and even returns the geolocations of hundreds of additional nearby BSSIDs. This behavior, while useful for speeding up location services, creates a serious privacy vulnerability. Anyone can systematically query the API using randomly generated or guessed BSSIDs (based on known manufacturer patterns), and Apple's system will return accurate geolocation data. In practice, this allows anyone with basic technical skills to build a near real-time map of Wi-Fi-enabled devices across the globe.

The Approach

The authors developed an automated system capable of generating plausible BSSID addresses by leveraging Organizationally Unique Identifiers (OUIs)-prefixes assigned to manufacturers of network devices. Using these OUIs, they were able to construct likely MAC address candidates and systematically submit them to Apple's Wi-Fi Positioning System (WPS) API. What made the attack particularly effective was not only that the API responded with the geolocation of known BSSIDs, but also that it opportunistically returned the locations of up to 400 nearby BSSIDs with each query. This feature, meant to improve location accuracy for mobile devices, inadvertently enabled attackers to expand their dataset exponentially with minimal effort.

Over a year, the researchers amassed geolocation data for more than 2 billion distinct BSSIDs. With this massive dataset, they were able to perform longitudinal analyses-tracking how access points moved geographically over time. This tracking revealed several compelling and concerning patterns. For instance, they observed the movement of personal and military devices into and out of conflict zones in Ukraine and Gaza, offering a form of open-source intelligence. In another case, they documented the disappearance of devices in the aftermath of the devastating Maui wildfires, reflecting areas of destruction. They also found that travel routers-such as those commonly used in RVs, military convoys, and refugee shelters-often moved across large distances, effectively tracing the movement of individuals or groups.

What is most troubling is that the vast majority of these tracked devices belonged to individuals who never gave explicit consent to participate in Apple's WPS. Many users were likely unaware that their Wi-Fi routers were being recorded and made remotely accessible through a third party's positioning system. Simply being within range of an Apple device was enough to have a router's location added to Apple's geolocation database-creating a silent but powerful surveillance network that users had no control over.

Hidden Threat of BSSID Persistence

A central enabler of this mass surveillance capability is the persistence of MAC addresses (specifically BSSIDs) which rarely change over time. While many modern smartphones randomize their MAC addresses to prevent long-term tracking, this privacy measure is not the norm among routers, IoT devices, or travel modems. These devices typically broadcast fixed identifiers, which means they can be observed and re-identified anywhere they are powered on. As a result, they become durable location markers like silent beacons that reveal their presence, movement, and behavior to any system listening.

This persistence creates especially dangerous consequences for vulnerable individuals and communities. Victims of domestic violence who relocate to escape abuse, displaced civilians fleeing war zones, journalists or activists operating under oppressive regimes, or military personnel deploying across

borders - all of these groups can be unintentionally exposed by something as simple as powering on a personal router. Once a persistent BSSID is associated with a particular person, behavior, or group, it can serve as a proxy for tracking them, even across countries and continents. In the hands of a malicious actor or even a curious observer, this data allows for profiling, location inference, and unwanted surveillance, all without consent or awareness from the affected parties.

Even more concerning is that this exposure can happen without any direct interaction with the Apple ecosystem. As the study demonstrates, merely being within the range of an Apple device is enough to have one's router captured and added to the WPS database. This means that people who do not own Apple products can still be included in the tracking system, without ever opting in or being notified. Persistent identifiers like BSSIDs are often treated as neutral technical details, but in a world where infrastructure quietly collects and shares this data, they become deeply personal and potentially harmful.

Discussion Questions

How does the passive nature of this surveillance affect public perception and accountability?. Unlike traditional surveillance systems that involve visible infrastructure, Apple's WPS operates invisibly through cameras, drones, or checkpoints. Data is collected passively, often without users' awareness or interaction, making the threat harder for the general public to grasp. Invisibility leads to a dangerous paradox: the more seamless and silent the data collection is, the less likely people are to recognize it as a violation. As a result, there's minimal public pressure on companies to improve safeguards. This situation fosters a lack of accountability; since there's no immediate sense of harm, affected individuals often don't even realize they've been exposed. In turn, regulators and lawmakers are less likely to prioritize such issues, allowing the system to persist largely unchallenged. This invisibility is precisely what makes it so effective and so insidious.

Could the normalization of geolocation tracking through services like WPS reshape our cultural expectations of privacy over time?. Yes, this process is already taking place. The subtle integration of systems like Apple's WPS into everyday life leads to a gradual erosion of what people expect privacy to mean. As geolocation tracking becomes a standard feature of smart devices, it shifts the cultural baseline: constant location awareness is increasingly seen as normal rather than invasive. This shift has long-term consequences. Younger generations may grow up believing that their physical movements are inherently observable, resulting in a diminished resistance to broader surveillance systems - whether public or corporate. Over time, this "new normal" poses a risk to essential social values such as anonymity, freedom of movement, and the right to disappear. Cultural shifts rarely happen suddenly; they unfold quietly, often through systems like WPS that operate outside the public's immediate awareness.

Conclusion

This case study clearly illustrates how a system built with good intentions, like Apple's Wi-Fi-based geolocation service, can be repurposed into a tool for mass surveillance when privacy is not a foundational consideration. The fact that anyone, without special privileges, can track devices across the world simply by guessing network identifiers is deeply concerning.

What makes this issue especially urgent is that it isn't just about technology but about ethics. It exposes a significant gap in how companies handle location data, often without the knowledge or consent of the individuals affected. These findings raise critical questions about transparency, accountability, and the right to privacy in public and private spaces alike.

As we continue to integrate digital tools into everyday life, it becomes increasingly important to demand systems that respect personal boundaries. Geolocation services, while useful, should never come at the cost of fundamental rights. This case reminds us that convenience, when unchecked, can quietly chip away at the freedoms we often take for granted.