An overview and analysis of Apple's AirTag technology and FindMy service

Zanolin Lorenzo

February, 2024

Contents

Abstract

The main goal of this project is to dig into how Apple AirTags work, including their setup, security measures, and uses; since everything is tied to the FindMy network and the UWB technology, we will also look into the security methods used in this network and the basic principle of the Ultra-Wideband (UWB). The idea is to get a clear picture of how Apple AirTags are put together, how secure they are, and the different ways they're used in the FindMy network.

1 Introduction

In the rapidly evolving landscape of technological advancements, Apple's AirTags have emerged as an innovation, offering a solution to tracking and locating personal belongings. This paper delves into the architecture and security of AirTags, with a particular emphasis on the UWB technology that underlies their functionality. Moreover, as AirTags operate within the framework of the FindMy network, this exploration extends to an overview of the security measures embedded in both the device and the overarching network; through the examination of the relationship between AirTags, UWB, and FindMy security, this paper seeks to provide insights of the working principles of the ecosystem which enables accurate location tracking, while also addressing concerns related to privacy and data security.

We will go over the fundamentals of UWB technology in Section 2 and examine its benefits from a security standpoint. In Section 3, we will delve deeper into the examination of the FindMy network. We will begin with providing a general overview of the architecture, go on to a functioning example and end with a security analysis of the whole thing. Lastly, we will conduct a thorough examination of the AirTag concept in Chapter 4, concentrating on the architecture (first examining the software component, then the hardware component) and then moving on to the security analysis of this technology.

2 UWB

2.1 Overview

Within the domain of wireless communication technologies, UWB operates by employing extremely low-power, short-duration pulses that span a broad spectrum and result in increased distance measuring precision, allowing for high data transfer rates and precise positioning capabilities over a wide frequency range, typically several gigahertz. Originally conceived for military and radar applications, it has gradually invaded diverse sectors, finding particular prominence in consumer electronics, healthcare, automotive systems, and the Internet of Things (IoT).

From [7]: "UWB achieves real-time accuracy because the receiver can determine the time of arrival of the signal, allowing centimeter-level accurate ranging using techniques such as Time-of-Flight (ToF)[1], Time Difference of Arrival (TDoA)[2] and Two-Way Ranging (TWR)[3]. Combining with error correction techniques, the ranging error can be as low as 58 mm".

Because of its wide spectrum utilization, UWB can coexist peacefully with other wireless technologies and send out massive volumes of data quickly; also, it has a reduced range of operation due to the wide radio bandwidth it uses (according to [36], "U1 chip can emit data using two frequencies: 6.24 GHz and 8.2368 GHz. The FCC has allocated ultrawideband a spectrum starting from 3.1GHz to 10.6GHz."). To overcome this problem, we can use an antenna of type *MIMO* (multiple-input and multiple-output) to enhance UWB's range; this kind of devices can be embedded into our everyday devices due to their reduced size. From [8]: "due to the low energy density and the pseudo-random (PR) characteristics of the transmitted signal, the UWB signal is noise-like which makes unintended detection difficult".

According to [3], "Apple-designed U1 chip uses UWB technology for spatial awareness, allowing iPhone 11, iPhone 11 Pro and iPhone 11 Pro Max or later iPhone models to precisely locate other U1-equipped Apple devices"; this means that when two U1 devices come close to each other, the two start measuring their exact distance using ToF. According to IEEE 802.15.4a [18], "UWB can determine the relative position of other devices in the line of sight even up to 200 meters", which means that we can leverage this technology to track items that are very close to us and those that are relatively distant.

It is important to distinguish the differences between Bluetooth Low Energy (BLE) and UWB. The former allows for detecting a device but cannot accurately measure its position, as it relies on the device's range. UWB, on the other hand, enables precise localization of the device by measuring the position based on the time it takes for the signal to travel from point A to point B. Table 1 represents the principal differences between the two technologies, data is taken from [9]:

Table 1: BLE-UWB comparison.

	UWB	**Bluetooth (BLE Beacons)**
Battery	Low consumption	Low consumption
Data Rate	1 Gbps	2 Mbps
Range	up to 200 meters	up to 100 meters
Accuracy	10 centimeters	up to a meter
Cost	Low	Depend on the context

[1]From [2], "Time of flight is the measurement of time taken to travel a distance in order to determine distance, speed, or properties of the medium".

[2]From [16], "TDoA is a positioning methodology that determines the difference between the time-of-arrival (ToA) of radio signals. TDoA is used in a real-time location system (RTLS) to accurately calculate the location"

[3]From [33], "The Two Way Ranging method determines the Time of Flight of the UWB RF signal and then calculates the distance between the nodes by multiplying the time by the speed of light."

2.2 Security analysis

The fact that UWB pulses are resistant to the multipath effect[4] is one of its key characteristics. This occurs when radio waves are reflected or refracted by artificial or natural objects near the primary signal channel, causing the signal to reach the receiver via many paths. Positioning accuracy is improved by immunity to the multipath effect, particularly when compared to other technologies that are more vulnerable. Moreover, UWB's resilience to jamming and narrowband fading makes it a particularly reliable technology choice, even when several UWB systems are being used at once.

Another important aspect to consider is the resistance to Relay Attacks, which is a vulnerability of the majority of signal-based architectures; we will present a concrete example taken from [12]. In this attack, the goal is to trick a car into thinking the key and owner are close by using two people with hacking devices. The first relays signals from the car to the second thief, who transmits the signal to the house. The key responds, allowing entry into the car. The relay attack intercepts and amplifies wireless signals used to unlock the door and start the car, despite the key's distance. With UWB, that would not be possible due to its working scheme: to ensure the car doesn't have to make assumptions, rapid measurements are utilized to establish distance very precisely. Any attempt to relay attack or intercept the UWB signal will merely cause the answering device's acknowledgement signals to arrive later, indicating to the car that the responding device is actually farther away rather than closer. The car's presumption is replaced with assurance when using UWB, which greatly increases the security of the passive keyless entry system.

The implemented security measures, taken by Apple, are the following: MAC address randomization and frame sequence number randomization [3].

2.2.1 MAC address randomization

From [3]: "Apple platforms use a randomized media access control address (MAC address) when performing scans when not associated with another device. Because a device's MAC address changes when disconnected from another device, it can't be used to persistently track a device by passive observers of traffic". This provides us with a level of protection against visibility from malicious individuals attempting to sniff the traffic for malicious purposes.

2.2.2 Frame sequence number randomization

From [3]: "Apple devices randomize the sequence numbers whenever a MAC address is changed to a new randomized address". As before, this addition increases the privacy, also avoid the possibility of replay attacks.

[4]From [10]: "Multipath interference occurs when a signal from a transmitter arrives at a receiver via two or more routes; typically there is a direct path plus a number of indirect paths caused by reflections".

3 FindMy network

3.1 Overview

Apple created the technology, known as the FindMy network, which is intended to assist consumers in finding their compatible third-party accessories, such as Apple AirTags, as well as their Apple devices, including iPhones, iPads, Macs, and AirPods. By utilizing UWB and BLE technologies, the FindMy network facilitates accurate and instantaneous location tracking.

Apple merged the applications Find My Friends and Find My iPhone together into a single app called *Find My*, allowing users to locate everything they need in one place. Subsequently, Apple has consistently enhanced the Find My app, incorporating functionalities such as monitoring when a iPhone is disconnected, when it is turned off and when it has been wiped.

You can access the sections of the app by touching the tabs located at the bottom. *People* are located on the left and represents your friends location (they have to share it with you in order to be visible), while your personal belongings, including Bluetooth goods with Find My functionality and AirTags, are located in the center; finally, on the right, there's a *Me* tab with all of your settings and info, as we can see in Figure 1.

There are several useful features within this app, we will present some examples taken from [6]:

- *Separation alerts*: you will get notified if you unintentionally leave behind an Apple device, an AirTag-tagged item or a third-party device that has enabled Find My features.

- *Locating friends and sharing location*: this feature allows you to share your location with friends or family so they can view it when needed. One useful aspect of this function is that it also enables you to monitor your children or individuals with certain orientation problems, helping them if they get lost.

- *Locating devices without connection*: this feature is very useful as it allows devices that are not connected to the Internet to be tracked using the FindMy network. Essentially, a lost device uses BLE to send beacon packets to nearby Apple devices, which then send the encrypted location to the owner's iCloud account. As we will see later, it will also be possible for some devices to be located even without battery charge, meaning when the device is turned off.

- *Anti-stalking measures*: this feature helps prevent situations where a malicious individual secretly places a device belonging to a FindMy network in your belongings to track your location in real time, using your device to upload its position. When your device receives multiple BLE beacons from a nearby device, it will notify you that you might be tracked by a device and ask if you want to disable its location sharing. We will also come back on this following the studies done in [13].

Figure 1: FindMy screenshots (images from [37]).

- *Precision finding*: this feature requires the presence of the U1 chip, which uses UWB technology to locate another device equipped with the same chip. It is very useful for precisely locating AirTags, which are often attached to items that we tend to lose frequently. The range of this technology is limited to that of UWB, as we previously discussed.

3.2 Functioning

Now, we will describe the entire functioning process. First of all, we want to register our products within the application; in the case of a non-accessory item, it will automatically be inserted in the *Devices* section. In the case of accessories, like AirTag, you need to manually add them using the *Items* section.

Now you should be able to localize online devices from the map; in the case of a close AirTag you can also use the *Precision finding* to locate the object using U1 chip, as represented in Figure 2. From [28]: “the technology fuses input from the iPhone’s camera, ARKit, accelerometer and gyroscope in order to guide the user to their AirTag using a combination of sound, haptics, and visual feedback.”

In case of a stolen device, you can always activate *Lost Mode*; it will send you a notification as soon as the iphone is detected, which means that if the phone is connected to a network or via BLE to other Apple devices, the owner will receive a message from FindMy containing the position of the device. Also, in this modality, all the registered cards in Apple Pay will be temporarily disabled.

This technology seems pretty useful already, but if a device is powered off, how can it be localized? If you device is U1-equipped, its Bluetooth is enabled

Figure 2: Precision Finding.

and its iOS version is at least 15 then it can be localized even if turned off. From [24]: "with iOS 15, your iPhone is still traceable through the Find My network even when the device is powered off. It seems that with iOS 15, the phone is not really fully powered off, it stays in a low-power state and acts like an AirTag, allowing any nearby iOS device to pick up the Bluetooth signal and send back its location. This also means if the iPhone runs out of battery during the day, the owner still has a chance of finding its location for several more hours. As long as Activation Lock is activated and the phone is restored to factory settings, Apple claims that location tracking will continue to function".This seems very useful for iPhones, but what about other devices, like Macbooks? Since Apple has not commented on the matter, the author conducted some tests and discovered that even machines with high specifications lack the U1 chip and are therefore not localizable when turned off.

As already written, all of the tracking capabilities that are available for Apple devices, such as iPhones and iPads, are also accessible for AirTags and may be tracked via the *Items* section. When AirTags are out of range of their owners' devices, they may be tracked by billions of iPhones, iPads, and Macs thanks to the Find My network and a Lost Mode. The only way to stop an AirTag from being fully detectable is to remove the CR2032 coin battery (or when it fully discharges).

3.3 Security analysis

In this section, we will analyze the security measures implemented in FindMy to increase the safety of the architecture. Let us add some more details to the process of localizing an object.

3.3.1 Preliminars definitions

We will first define a few terms taken from [14]:

- *Owner Devices*: owner devices linked to a shared Apple ID can utilize the Find My application across macOS, iOS and iPadOS to locate any devices associated with the same owner.

- *Lost Devices*: when devices are deemed lost, they begin broadcasting BLE advertisements containing a public key, which can be detected by finder devices. Apple devices are classified as lost when they lose internet connectivity. Third-party accessories [30] are compact, battery-powered devices that can be affixed to personal items and are configured via the owner's device. Accessories are considered lost when they lose their BLE connection to the owner's device.

- *Finder Devices*: the FindMy network is supported by Finder devices. By 2023, the only iPhones and iPads with a GPS module will be able to use a finder. By looking for BLE ads, finder devices can identify misplaced gadgets and accessories. A finder device sends an end-to-end encrypted location report, including its current location, to Apple's servers after intercepting an advertisement. We will see what the contents of the report are.

- *Apple's Servers*: the location reports that finding devices send are stored on Apple's servers and only owner devices are able to retrieve and locally decrypt those information.

3.3.2 Workflow

From [3], page 202: An online device can report its location to the user via iCloud. Find My works offline by sending out short range BLE signals from the missing device that can be detected by other Apple devices in use nearby. Those nearby devices then relay the detected location of the missing device to iCloud so users can locate it in the Find My app while protecting the privacy and security of all the users involved. An example of the previous workflow is represented in Figure 3.

All finder devices regularly scan for FindMy advertisements. The finder creates and uploads an encrypted position report to Apple's servers whenever it receives a packet in the FindMy advertising format. Finder devices are likely to use less energy and bandwidth because they gather reports over time and transfer them in batches on a regular basis. The evaluation done in [14] discovered that the median time from generating to uploading a location report is 26 minutes and the delay can increase to several hours if the finder device is in low power mode.

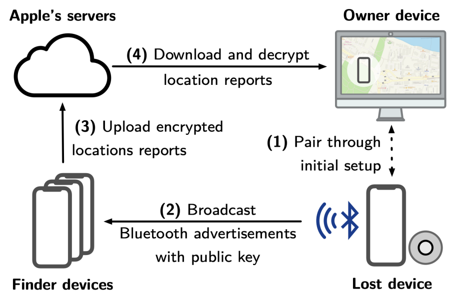

Figure 3: FindMy workflow (image from [14]).

3.3.3 Cryptography

We will now delve more into the Cryptography protocols used.

3.3.3.1 Advertisement keys

FindMy utilizes Elliptic Curves [25]; according to [3, 14], the process to generate *advertisement keys* is the following:

1. Each owner device generates a private/public key pair (d_0, p_0) on the NIST $P-224$ curve and a 32-byte symmetric key SK_0 that together form the master beacon key. Those keys are never sent out via BLE and are used to derive the rolling advertisement keys included in the BLE advertisements. Note that device tracking is hard since rolling keys can be deterministically derived if and only if one knows the initial input keys (d_0, p_0) and $SK0$.

2. Advertisement keys (d_i, p_i) are iteratively calculated as follows using the ANSI X.963 key derivation function KDF [1] with $SHA-256$ [11] and a generator G of the NIST P-224 curve:

$$SK_i = KDF(SK_{i-1},\ 'update',\ 32) \tag{1}$$
$$(u_i, v_i) = KDF(SK_i,\ 'diversify',\ 72) \tag{2}$$
$$d_i = (d_0 * u_i) + v_i \tag{3}$$
$$p_i = d_i * G \tag{4}$$

   where Equation (1) derives a new symmetric key from the last used symmetric key with 32 bytes length. Equation (2) derives the so-called "anti-tracking" keys u_i and v_i from the new symmetric key with a length of 36 bytes each. Finally, Eqs. (3) and (4) create the advertisement key pair via EC point multiplication using the anti-tracking keys and the master beacon key d_0.

3.3.3.2 Key synchronization

To download and decode location information, the advertisement keys must be accessed by all owner devices. In order to synchronize the master beacon keys, FindMy uses iCloud to encrypt a property list file in the Galois/Counter mode of the Advanced Encryption Standard (AES-GCM) [19]. The file's decryption key is kept in the iCloud keychain underneath the label "Beacon Store".

3.3.3.3 Encryption

The BLE advertisements sent out by a lost device contain an EC public key p_i. When a finder device sees one of these advertisements, it uses p_i to encrypt its current position and determines it. OF uses the Elliptic Curve Integrated Encryption Scheme (ECIES), which generates a shared secret that is utilized to encrypt the report through an ephemeral Elliptic Curve Diffie-Hellmann (ECDH) key exchange. According to [14], the finder's encryption algorithm works as follows:

1. Generate a new ephemeral key (d', p') on the NIST P-224 curve for a received FindMy lost advertisement.

2. Perform ECDH using the ephemeral private key d' and the advertised public key p_i to generate a shared secret.

3. Derive a symmetric key with ANSI X.963 KDF on the shared secret with the advertised public key as entropy and SHA-256 as the hash function.

4. Use the first 16 bytes as the encryption key e'.

5. Use the last 16 bytes as an initialization vector IV.

6. Encrypt the location report under e' and the IV with AES-GCM.

The ephemeral public key p' and the authentication tag of AES-GCM are part of the uploaded message. All location reports are identified by an ID which is the SHA-256 hash of p_i, as we can see in Figure 4.

3.3.3.4 Decryption

An owner device that downloads encrypted location reports follows the inverse of the encryption procedure:

1. The owner device selects the proper advertisement keys (d_i, p_i) based on the hashed p_i of the location report.

2. It performs the ECDH key exchange with the finder's ephemeral public key p' and the lost device's private key d_i to compute the symmetric key e' and the IV.

3. Now, the owner can use e' and IV to decrypt the location report.

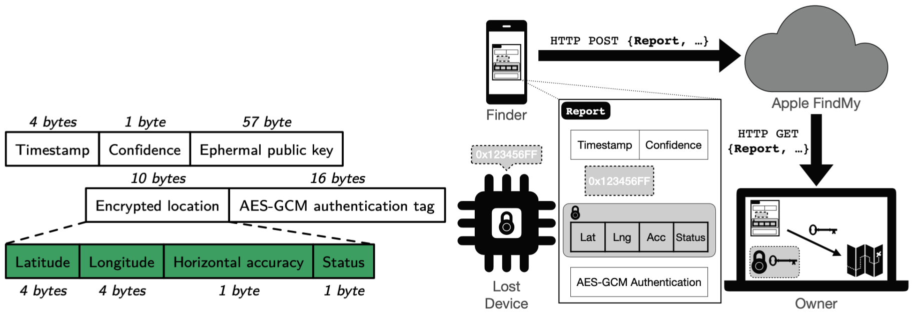

Figure 4: (a) Binary format of a location report (b) Example of sent payload (images from [14],[13]).

4 AirTag

An AirTag is a small tracking device developed and sold by Apple; it is intended to assist users in finding and monitoring objects that are easily misplaced or lost, such as wallets, bags, and keys.

4.1 Overview

By connecting to compatible Apple devices (iPhones, iPads, and Macs) through Bluetooth, the AirTag enables users to locate the linked object and, subsequently, the AirTag itself using the Find My app. In order to help with lost item recovery, the gadget has capabilities including accurate location tracking, proximity notifications and a Lost Mode. Its design prioritizes privacy and security, safeguarding user data through the use of encryption and anonymization. Support for the AirTag was introduced in iOS 14.5 and Apple lists as compatible all the devices that support iOS 14 and iPadOS.

4.2 Architecture

First of all, we will analyze the architecture of this product; the information has been reverse engineered by Adam Catley in [4]. We will cover both the hardware and software aspects of this kind of device.

4.2.1 Software analysis

As for the software part, we will present informations taken from [4]. Adam Catley identified various states in which AirTag can be; we will now quickly present all of them.

- *Not registered*: when removed from FindMy network or reset, the AirTag is brand new and every 33 milliseconds, it advertises itself as it waits to be connected.

- *Initialisation*: a public/private key pair is created and shared by the AirTag and the linked iOS device after it is registered to an Apple ID.
- *Connected*: the owner's device is in range. No broadcasts occur.
- *Disconnected*: the owner's device is out of range. Broadcasts identity every 2000 ms.
- *Out of sync*: happens when an AirTag reboots while separated from its owner's device. Acts like Disconnected but absolute time is lost, so events are relative to time since power-up. Identity resets to its initial value.
- *Lost*: occurs 3 days after Disconnected or Out of sync begins. Moves to Waiting for motion every 6 hours.
- *Waiting for motion*: samples the accelerometer every 10 seconds until motion is detected.
- *Sound alert*: a command to play a noise is received from either a connected device or by detecting motion. Lasts a maximum of 20 seconds.
- *Precision finding*: triggered by the owner's device while Connected. Is overridden by Sound alert.

As we will see in Section 4.2.2, even if the finder has an Android device, they may be able to identify the owner of an AirTag thanks to its NFC antenna. Depending on its current status, the tag carries a URL that uniquely identifies the AirTag. It can only be read when the AirTag is powered by a battery. There are some parameters that are attached to the URL, used to identify the device; we will briefly present them. These informations were presented in [4]. Keep in mind that all of the following parameters are fixed for a single unit, even after power cycles, long runtime, resets and modes.

- *pid*: product ID for AirTag.
- *b*: something related to the battery.
- *pt*: UWB Precision Tracking version.
- *fv*: firmware version.
- *dg*: something related to diagnostic.
- *z*: unknown.
- *bt*: Bluetooth address; will be present only when Unregistered.
- *st*: serial number of the tag (the one printed on the device under the battery); will be present only when Unregistered.
- *bp*: Bluetooth protocol version; will be present only when Unregistered.

In the **Unregistered** state, the stored URL has the following format: `https://found.apple.com/airtag?pid=5500&b=00&pt=004c&fv=00100e10&dg=00&z=00&bt=A0B1C2D3E4F5&sr=ABCDEF123456&bp=0015`

Once the device is **registered**, the parameters *bt, sr, bp* will be removed and replaced with a single anonymous identifier *pi*, which is the only parameter that changes at least every 15 minutes when the Bluetooth address and/or the advertising data changes. It is likely the current P-224 public key p_i presented in 3.3.3.1 or the SHA-224 of it.

The device operates on a schedule designed to optimize its functionality: at 4:00 am every day, it updates its BLE address and public key, ensuring secure communication channels. Advertisement data is refreshed every 15 minutes, guaranteeing that nearby devices receive the most current information. Should it become separated from its owner's device for three days, the device enters a lost mode, activating specific features to aid in recovery efforts. While in this lost mode and detecting movement, the device emits a noise every 6 hours to alert nearby individuals. To conserve energy while remaining responsive, the accelerometer is sampled every 10 seconds when waiting for movement. Upon detecting motion, the accelerometer sampling frequency increases to every 0.5 seconds for 20 seconds, providing detailed tracking data. When away from its owner's device, the device transmits BLE advertisement signals every 2 seconds, enhancing its detectability. Finally, in close proximity to its owner's device, the device establishes a BLE connection interval of 1 second, ensuring efficient communication and responsiveness.

4.2.2 Hardware analysis

As for the hardware part, an important aspect comes to light: all of the used components, apart from Apple's U1 UWB chip, are off the shelf, as we can see in Figure 5. Each AirTag has three antennas: one for BLE that works at 2.4 GHz, one for NFC at 13.56 MHz and finally the UWB one at 6.5-8 GHz. The outer plastic shell, which serves as a diaphragm, is adhered to the voice coil. When the coil is energized, the fixed magnet causes it to move back and forth, creating sound and serving as the speaker. Whether the voice coil is connected or not, the AirTag functions in the same way. If motion is detected, the speaker will loudly beep for up to 20 seconds after being away from its owner's device for three days. After that, it will be silent for the following six hours before watching for movement once more.

4.3 Security Analysis

Security-wise, there is a lack of basic security controls in this kind of device; in fact, none of the data in the AirTag is protected from tampering or disclosure.

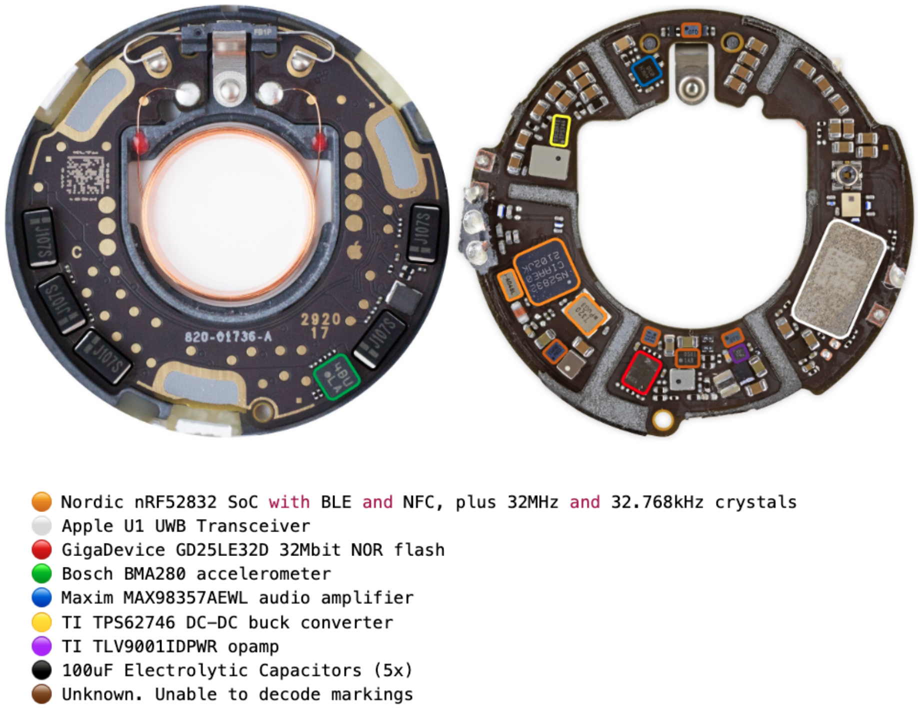

Figure 5: PCB overview (image from [4]).

4.3.1 Vulnerabilities

We will present some vulnerabilities that have been found by by Adam Catley in [4]; Table 2 resumes them.

4.3.1.1 Exploitable voltage levels

The Nordic nRF52832 has the function Access Port Protection [32] that is used to disable access to the Debug Port through SWD and prevent reading out the internal memory; however, according to [31], this mechanism is vulnerable to side channel attacks and can be bypassed through voltage glitching. Consequentially, it is possible to extract Bluetooth pairing keys to connect to the owner's phone or run (on the AirTag) a custom firmware since Apple does not check the signature of it (the firmware). In this case, if an attacker is able to use voltage glitching to inject a modified firmware, maybe he can use it to track the owner and it will not be discovered since the anti-stalking countermeasures presented in 4.3.2 do not work with personal objects. According to [15], the only way to guarantee the security of the voltage glitch detection circuitry protecting an SoC or microcontroller is to implement the detector on the chip itself. An example of detector is Voltage Glitch Detector IP from INVIA, which provides comprehensive protection against power glitching attack. It detects positive and negative supply voltage glitches, and has a slope detection range between 100 MV/s and 2 GV/s.

4.3.1.2 Insecure Storage

The GD25LE32D 32Mbit NOR flash is not encrypted, as we can see in [27]; also, the nRF52832 does not have any secure storage functionality. In this case, we don't know if this is a real vulnerability since we do not know whether the FindMy private key-pair is stored inside the AirTag. However, an attacker can read without problems all the information that is stored within the device and, in general, this behavior can be exploited (maybe in the future) to inject malicious data into the AirTag or to read sensible informations. To prevent this, we can implement encryption via software or hardware; typically, on small devices, it is better to use dedicated hardware circuitry to encrypt data.

4.3.1.3 Unathenticated transmission

The only way to identify an AirTag is to use its public key, which is transmitted via BLE advertising packets; this identification does not require authentication. These IDs can be recorded and replayed by any nearby BLE device to mimic the appearance of the real AirTag. Let's see an example taken from [4]: an attacker steals a personal item containing an AirTag and subsequently records the current public identity before removing the battery. At this point, the identity can be relayed to any BLE device in a decoy location to give the owner a false search area to recover their property. In this case, the AirTag is exploited to steal personal belongings from the owner. To avoid this, Apple can use authenticated encryption; for example, we can use GCM, which offers the ability to verify the authenticity and integrity of extra authenticated data (AAD) that is provided in clear text in addition to authenticated encryption (confidentiality and authentication). More details can be found in [19].

Table 2: Vulnerabilities.

Vulnerability	**Possible attack**	**Countermeasure**
Exploitable voltage levels	Side-channel attack	Use detector
Insecure storage	Memory-reading attack	Implement hardware encryption
Unauthenticated transmission	Replay attack	Implement authenticated encryption

4.3.2 Anti-stalking countermeasures

An important aspect that has emerged with the AirTags is the stalking problem. Stalking using AirTags refers to the potential misuse of Apple's AirTag tracking devices to monitor and track individuals without their consent; these small devices are designed to help users locate misplaced items. However, due to their small size and long battery life, AirTags could potentially be used for nefarious purposes, such as stalking. An individual could secretly place an AirTag on someone's belongings and then use the Find My app to monitor their movements in real-time. Since AirTags are designed to be difficult to detect, the victim may not realize they are being tracked for an extended period of time.

Apple has implemented measures to prevent the misuse of AirTags, including alerts and notifications for when an unknown AirTag is detected near a user's device, as well as features like Precision Finding, which can help users locate unwanted AirTags. The first line of defense in the event that someone plants an AirTag on a victim's belongings might be an alert to his iPhone indicating the presence of a foreign AirTag. Apple built the iPhone-AirTag connection to do this in two ways: either when you get to the place that your iPhone's machine learning intelligence has detected as home (or when you manually record it as home) or after the AirTag has stuck with you for a certain "continuous" period of time that Apple deems sufficient to be considered abnormal. This seems perfect; however, if the victim has a non Apple device, such as an Android phone this could be a problem. To prevent this problem, Google and Apple collaborated to develop Unknow Tracker Alerts, which is a feature that was announced during the Google I/O 2023 opening presentation.

Furthermore, AirTags are made to make noise if they are absent from their owner for a long time, which could potentially notify the victim that a tracking device is present. More precisely, three days following separation is when sound alerts begin; even in that case, they only occur once motion is identified and only for a maximum of 20 seconds. After that, the AirTag remains silent for a maximum of 20 seconds every six hours while it waits for movements. As correctly observed by Catley in [4], the problem with this is that three days can be enough to study the victim's routine and after that period, it is likely to make noise for a maximum of 40 seconds a day during a normal commuting schedule. Movement is likely to coincide with a noisy environment while traveling or be muffled by objects touching the white casing, meaning that the victim won't realize it. According to [26], the frequency and duration of sounds can be adjusted from the Apple server side, meaning that Apple can increase both of them to avoid situations in which the victim is unable to hear the sounds.

However, despite these safeguards, the potential for AirTags to be used for stalking remains a concern; in fact, a problem is that the voice coil can be disconnected without disassembly. As a result, an attacker can easily alter an AirTag and place it unintentionally in someone's possessions to track a target's whereabouts without the victim being aware of it vocally. The AirTag will continue to operate normally in this manner without making any noises.

4.4 Useful applications

Some useful applications can be the following:

- *Travel*: AirTags can be beneficial for travelers. They can attach AirTags to their luggage, making it easier to identify and track their bags during travel. As example, imagine you have just landed from a trip and are eager to grab your bags, waiting endlessly at the carousel can be frustrating. You start worrying that your luggage got lost, but if you've got AirTags inside, you can quickly check if it's still at the airport or somewhere else. Even if it's taking longer than expected, you can keep tabs on it until the airline sorts things out and gets it back to you.

- *Pet Tracking*: while not explicitly designed for pets, some users have found AirTags useful for tracking their pets. By attaching an AirTag to a pet's collar, owners can monitor their pet's location and quickly locate them if they wander off. Some tests were conducted in [21] and, as we could expect, it seems that the AirTag doesn't work quite well when in motion, for example, on a moving cat. In [34], they conducted a test trying to track a dog. As before, the experiment was delusional; they tried to simulate the dog using a plastic box that contained the AirTag and was dropped near a spot where dog walkers regularly walk past it every day. Several hours passed before the user received the initial location fix for the lost AirTag. However, this fix was a singular occurrence, and there was no subsequent update for several more hours.

- *Child Safety*: similarly to pets, AirTags can give an extra degree of protection for monitoring kids in busy or strange places. An AirTag can be attached to a child's clothing item or backpack, allowing parents to track their movements and get notifications if the youngster ventures too far. From [20]: ethical debates can arise regarding this issue, as experts have long been worried about the impact of more restrictive parenting on children's mental health and development. We will not go any deeper on this question since it is a technical report.

- *Vehicle Tracking*: AirTags can also be used to track vehicles, such as bicycles, motorcycles or cars, in the same way as the two above. An experiment was done in [23] where an Apple AirTag, a Samsung SmartTag+, and a GPS unit with 3G and 4G compatibility were used to evaluate their performance and determine the most cost-effective solution to track a device; additionally, as a backup measure to these external devices, they used the ConnectedDrive feature on a BMW 3 Series to compare its effectiveness against the other options. Table 3 compares the cost of the used options, data is taken from [23]. The testing route consists of a 45 km drive and includes four checkpoints. There is no LTE or cell service in close proximity of the last checkpoint; after going back to the starting point, the test ends by evaluating how well each gadget finds the parked automobile once it is in range and idly. The results were as assumed: both aftermarket and built-in GPS units were expected to function properly, transmitting accurate locations via cellular networks, facilitating easy vehicle tracking; however, their main drawback is their cost and the need for ongoing battery monitoring or charging to ensure continuous functionality. In terms of

Figure 6: Unremovable bracelet (image from [35]).

UWB, the AirTag proved to be a reliable and affordable option for tracking the car in the event of theft, even though it didn't provide updates as often as the SmartTag+.

Table 3: Solutions cost comparison.

Device	**Cost ($AUD)**
Apple AirTag	$45
Samsung SmartTag+	$60
GPS tracker with SIM card	$147 + $7 per month
BMW ConnectedDrive	From $119 per year

- *People with Dementia Tracking*: Alzheimer's patients and those suffering from other types of dementia may notice a reduction in their memory for familiar locations, which can result in wandering and feelings of being lost or confused. AirTags can offer comfort in these situations and assist caretakers in making sure the person's whereabouts are known; some bracelets have been developed to facilitate the use of Airtags in this context. As we can see in Figure, the Unremovable Bracelet is used to track every movement and it takes two hands to open it, thus making it impossible for your loved ones to take it off.

- *Intrusion detector*: an innovative usage can be as an intrusion detector. Imagine a scenario where you want to check whether anyone is near your remote cabin; if you place an AirTag hidden somewhere near it, if someone with an iPhone passes nearby, then you will be noticed in minutes, since the intruder's device will forward to iCloud the AirTag position.

- *Wallet tracker*: this can be the most obvious application of this kind of device. A lot of wallets with built-in space for the AirTag were created, making it easier for the user to track their wallets.

- *Supermarket shelf localizer*: an interesting usage can be to act as a localizer inside a supermarket. Imagine a scenario where an elderly person goes grocery shopping in a very large supermarket and gets lost inside. In such cases, an application could be developed using Apple's APIs to help

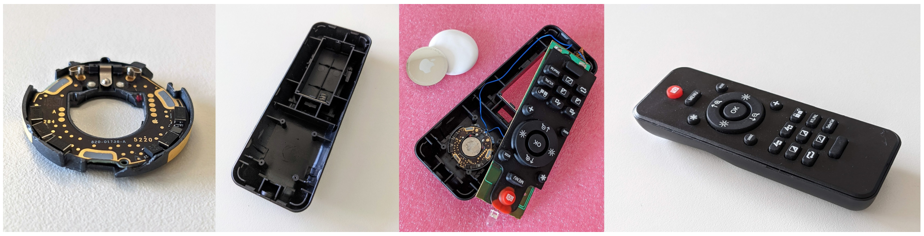

Figure 7: AirTag inside a remote control (images from [4]).

locate all the shelves for the user, utilizing the precision finding offered by UWB. In the future, integrated tablets could be available on shopping carts, allowing users to locate shelves using navigation (Precision Finding) provided in FindMy.

4.5 Mods

After some Internet research, the author discovered that the AirTag has been modified in certain ways. For instance, in [5] A. Catley has attached the AirTag to a remote controller and is powering the AirTag components using the host's battery. This could be very useful in situations in which the remote controller gets lost in the house; thanks to Precision Finding, the owner can find it easily. Figure 7 shows the final result. Now, imagination knows no bounds, and there are always innovative ways to utilize AirTags.

5 Conclusion

In conclusion, the paper provided a comprehensive exploration of various technological aspects. The AirTag technology and FindMy architecture offer a smart solution to address the tracking issue by intelligently utilizing the network of Apple devices worldwide, all at a much lower price compared to competitors.Other technologies also utilize the same principle, but AirTag's strength lies in the Apple device network present worldwide. Currently, according to [22], Apple holds 29.27% of the smartphone market share. This explains why the service performs so well. There are numerous possibilities for the future, some of which have been discussed in Section 4.4. One potential future development of this technology could involve integrating it into everyday tools to add precision tracking capabilities. For instance, integrating FindMy into shopping carts in supermarkets to locate shelves. In the future, this technology can only improve as the network of Apple devices supporting both FindMy and Precision Finding continues to grow with the purchase of new iPhones (which now integrate the UWB chip). Security-wise, vulnerabilities highlighted in Section 4.3.1 need to be addressed, as user privacy is paramount, and a company like Apple cannot afford to ignore the issue.

References

[1] en. URL: https://csrc.nist.gov/CSRC/media/Events/Key-Management-Workshop-2000/documents/x963_overview.pdf.

[2] en. URL: https://www.analog.com/en/resources/glossary/time-of-flight.html.

[3] Apple. *Apple Platform Security*. en. May 2022. URL: https://support.apple.com/en-gb/guide/security/welcome/web.

[4] Adam Catley. *Apple AirTag Reverse Engineering - Adam Catley*. en. URL: https://adamcatley.com/AirTag.html#pcb-overview.

[5] Adam Catley. *Tweet by Adam Catley*. May 2021. URL: https://twitter.com/adamcatley/status/1393171134489808896.

[6] Juli Clover. "Find my App: Everything to Know". en-US. In: *MacRumors* (Feb. 2022). URL: https://www.macrumors.com/guide/find-my/.

[7] Dieter Coppens et al. "An Overview of UWB Standards and Organizations (IEEE 802.15.4, FiRa, Apple): Interoperability Aspects and Future Research Directions". In: *IEEE Access* 10 (2022), pp. 70219–70241. ISSN: 2169-3536. DOI: 10.1109/access.2022.3187410. URL: http://dx.doi.org/10.1109/ACCESS.2022.3187410.

[8] Maria-Gabriella Di Benedetto. "UWB communication systems: a comprehensive overview". In: (2006).

[9] Encstore. *BLE vs UWB: What Are the Differences*. s.d. URL: https://www.encstore.com/blog/5524-ble-vs-uwb-what-are-the-differences.

[10] Chad Figueroa. *What does antenna diversity do? Durrell2012.com*. en-US. Sept. 2022. URL: https://durrell2012.com/what-does-antenna-diversity-do/.

[11] Henri Gilbert and Helena Handschuh. "Security analysis of SHA-256 and sisters". In: *International workshop on selected areas in cryptography*. Springer. 2003, pp. 175–193.

[12] Deb Spitler Hid Global. *Applying Ultra-Wideband wireless technology for security and automation*. en-US. Nov. 2020. URL: https://www.securityindustry.org/2020/11/17/applying-ultra-wideband-wireless-technology-for-security-and-automation/.

[13] Alexander Heinrich, Niklas Bittner, and Matthias Hollick. "AirGuard-protecting android users from stalking attacks by apple find my devices". In: *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2022, pp. 26–38.

[14] Alexander Heinrich et al. "Who Can Find My Devices? Security and Privacy of Apple's Crowd-Sourced Bluetooth Location Tracking System". In: *CoRR* abs/2103.02282 (2021). arXiv: 2103.02282. URL: https://arxiv.org/abs/2103.02282.

[15] *How a voltage glitch attack could cripple your SoC or MCU - and how to securely protect it*. en. URL: https://www.design-reuse.com/articles/48553/how-a-voltage-glitch-attack-could-cripple-your-soc-or-mcu.html.

[16] Inpixon. *Time Difference of Arrival (TDOA) multilateration — INPIXON*. en. URL: https://www.inpixon.com/technology/standards/time-difference-of-arrival.

[17] Mahmoud Itani. *How are iPhones still findable even when turned off*. en. Oct. 2021. URL: https://www.xda-developers.com/iphone-findable-turned-off/#:~:text=Most%20time%2C%20U1%20is%20on,the%20connected%20device%20via%20Bluetooth..

[18] Eirini Karapistoli et al. "An overview of the IEEE 802.15.4a Standard". In: *IEEE Communications Magazine* 48.1 (2010), pp. 47–53. DOI: 10.1109/MCOM.2010.5394030.

[19] Emilia Käsper and Peter Schwabe. "Faster and timing-attack resistant AES-GCM". In: *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer. 2009, pp. 1–17.

[20] Heather Kelly. "Parents are using AirTags to track kids and give them freedom". en. In: *Washington Post* (Aug. 2023). URL: https://www.washingtonpost.com/technology/2023/07/26/tracking-kids-airtags/.

[21] Emily - KittyCatGO. *The Apple AirTag for Cats: A pet tracking review*. en-US. Mar. 2024. URL: https://kittycatgo.com/the-apple-airtag-for-cats-a-pet-tracking-review/.

[22] Ying Lin. *Smartphone Market Share Worldwide [Feb 2024 Update]*. en-US. URL: https://www.oberlo.com/statistics/smartphone-market-share.

[23] Paul Maric. "How to keep track of your car with these cheap devices: AirTag v SmartTag+ v GPS — CarExpert". enAU. In: *CarExpert* (Mar. 2023). URL: https://www.carexpert.com.au/car-comparisons/stolen-car-these-cheap-devices-will-track-it-airtag-smarttag-and-gps-tracker.

[24] Benjamin Mayo. *iOS 15: Find My network can still find your iPhone when it is powered off, or factory reset - 9to5Mac*. en-US. June 2021. URL: https://9to5mac.com/2021/06/07/ios-15-find-my-network-can-find-your-iphone-when-it-is-powered-off/.

[25] Victor S Miller. "Use of elliptic curves in cryptography". In: *Conference on the theory and application of cryptographic techniques*. Springer. 1985, pp. 417–426.

[26] Dan Moren. *The Fine Print on Apple's AirTags*. Apr. 2021. URL: https://daringfireball.net/linked/2021/04/20/moren-fine-print.

[27] Ghidra Ninja. *Tweet by Ghidra Ninja*. May 2021. URL: https://twitter.com/ghidraninja/status/1390619216823390208.

[28] Britta O'Boyle. *What is Precision Finding on AirTags and how does it work?* en. Nov. 2021. URL: https://www.pocket-lint.com/phones/news/apple/156605-what-is-precision-finding-on-apple-airtags-and-how-does-it-work/.

[29] Jake Peterson. *20 surprisingly practical uses for Apple AirTags*. en. Dec. 2022. URL: https://ios.gadgethacks.com/how-to/20-surprisingly-practical-uses-for-apple-airtags-0384571/.

[30] Apple Inc. All rights reserved. *MFi Program - create accessories that communicate with Apple devices using MFi technologies and components*. en. 2023. URL: https://mfi.apple.com/.

[31] Limited Results. *nRF52 Debug Resurrection: Approtect Bypass*. June 2020. URL: https://limitedresults.com/2020/06/nrf52-debug-resurrection-approtect-bypass/.

[32] Nordic Semiconductor. *Nordic Semiconductor Infocenter*. s.d. URL: https://infocenter.nordicsemi.com/index.jsp?topic=%2Fps_nrf52833%2Fdif.html&anchor=concept_udr_mns_1s.

[33] Milan Simek. *Two Way Ranging (TWR) - SeWiO RTLS*. en-US. Jan. 2024. URL: https://www.sewio.net/uwb-technology/two-way-ranging/.

[34] Src. *Can I use an AirTag to track my dog?* en-GB. Mar. 2024. URL: https://www.pitpat.com/doggy-products/can-i-use-an-airtag-to-track-my-dog/.

[35] *Unremovable AirTag® bracelets*. en. URL: https://www.medicalidfashions.com/Unremovable%20AirTag%20Bracelets.

[36] Ramish Zafar. "iPhone 11's U1 Chip Uses 6Hz & 8GHz Frequencies In UWB Spectrum". en-US. In: *Wccftech* (Nov. 2019). URL: https://wccftech.com/iphone-11-u1-chip-uwb/.

[37] Christian Zibreg and Christian Zibreg. "How to add third-party accessories to Apple's Find My app to keep track of them". en-US. In: *iDownloadBlog.com* (Apr. 2021). URL: https://www.idownloadblog.com/2021/04/09/add-third-party-find-my-accessories-tutorial/.