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, allowing for high data transfer rates and precise positioning capabilities. 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).

The unique feature of UWB is its capacity to send information across a large frequency range, usually several gigahertz; a UWB transmitter sends billions of radio pulses across the wide spectrum frequency and a UWB receiver then translates the pulses into data. The shorter the duration of the impulse, the

more precise the distance measurement will be. According to [6], 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), Time Difference of Arrival (TDoA) and Two-Way Ranging (TWR). 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. Since its ability to transmit informations across a wide radio bandwidth, from 500 MHz to several gigahertz, this technology has a short range of operation. According to [7], 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. To increase UWB's range and reception reliability, a *MIMO* (multiple-input and multiple-output), distributed antenna system has been added to the standard that enables short-range networks. The antennas can be embedded into a smartphone or other devices such as a wristband or smart key.

According to [2], 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. When two U1 devices come close to each other, the two start measuring their exact distance. The ranging is accomplished through Time of Flight (ToF), which is the time it takes for a pulse to get from point A to point B. According to IEEE 802.15.4a [13], UWB can determine the relative position of other devices in the line of sight even up to 200 meters.

A difference w.r.t. Bluetooth Low Energy (BLE) is that with BLE you can't really measure location or distance. What you can do is detect if a device like a smartphone is within range of another device. UWB, in comparison, provides much higher accuracy (up to a few centimeters). In contrast to BLE, the distance it measures is not based on the signal strength, but on the time it takes the signal to travel from point A (smartphone) to point B (UWB tag). Table 1 represents the principal differences between the two technologies, data is taken from [8]:

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

3

2.2   Security analysis

The fact that UWB pulses are resistant to the multipath effect[1] 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. Within these attacks, the goal is to trick a car into thinking the key and owner are close by using two people with hacking devices [21]. 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 UWB-based lock and ignition 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 [2].

2.2.1   MAC address randomization

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.

2.2.2   Frame sequence number randomization

Apple devices randomize the sequence numbers whenever a MAC address is changed to a new randomized address.

---

[1]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.

Because it may be used to find everything you need, Apple combined the Find My Friends and Find My iPhone apps into a single one that is simply called *Find My*. 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.

The app is organized into several sections, accessible by tapping the tabs at the bottom. On the left, you can find people, in the middle, you can find your own devices and items, such as AirTags and Find My-enabled Bluetooth items; 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, as an example:

- *Separation alerts*: designed to let you know if you leave an Apple device, a device attached to an AirTag, or a Find My-enabled third-party device behind.

- *Locating friends and sharing location*: implemented to locate friends and family members that have shared their location with you. You can view their location using the *People* tab within the Find My app.

- *Locating devices without connection*: let your lost devices be located even when not connected to WiFi or LTE by leveraging BLE and proximity to other nearby Apple devices. When your lost device is offline but close to another one, it's able to connect to that other device over Bluetooth and relay its location. We will come back on this.

- *Anti-stalking measures*: designed to let you know if there's a Bluetooth item near you. You will receive a notification when an unknown item is found and moving with you, so you can make sure no one slips an AirTag or other Find My Bluetooth devices into your things to track you. We will also come back on this following the studies done in [10].

- *Precision finding*: takes advantage of the U1 chip within AirTags and the iPhone 13, iPhone 12 and iPhone 11 models. Apple's U1 chip uses UWB to precisely locate and communicate with other U1-equipped devices, enabling AirTags and iPhones to work together.

Figure 1: FindMy screenshots.

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. 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? With the introduction of iOS 15 and the U1 chips, Apple claimed that even a U1-based iPhone can be localized even when turned off if and only if Bluetooth is turned on. From Apple: 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. In fact, Apple says the location tracking will

Figure 2: Precision Finding.

even keep working while the phone is reset to factory settings with Activation Lock enabled. 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, AirTags can be tracked through the *Items* tab and have all of the tracking features available to Apple devices like iPhones and iPads. There's a Lost Mode, and AirTags can also take advantage of the Find My network that allows them to be tracked by billions of iPhones, iPads, and Macs when they're out of range of the owner's devices. 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

Let us first define a few terms in accordance with [11]:

- *Owner Devices*: owner devices share a common Apple ID and can use the Find My application on macOS, iOS and ipadOS to search for any devices of the same owner.

Figure 3: FindMy workflow (image from [11]).

- *Lost Devices*: devices that are determined to be in a lost state start sending out BLE advertisements with a public key to be discovered by finder devices. Apple devices are considered to be lost when they lose Internet connectivity. Third-party accessories [22] are small battery-powered devices that can be attached to a personal item and are set up through an owner's device. Accessories determine to be lost when they lose their BLE connection to the owner's device.

- *Finder Devices*: finder devices form the core of the FindMy network. As of 2023, only iPhones and iPads with a GPS module will offer finder capabilities. Finder devices can discover lost devices and accessories by scanning for BLE advertisements. Upon receiving an advertisement, a finder creates an end-to-end encrypted location report that includes its current location and sends it to Apple's servers. We will see what the contents of the report are.

- *Apple's Servers*: Apple's servers store the location reports submitted by finder devices; only owner devices can fetch those reports and decrypt them locally.

3.3.2 Workflow

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 [11] 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.

3.3.3 Cryptography

We will now delve more into the Cryptography protocols used.

3.3.3.1 Advertisement keys

FindMy utilizes Elliptic Curves [17]; according to [2, 11], 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 $SHA - 256$ [9] 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) [14]. 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. A finder device that receives such an advertisement determines its current

location and encrypts the location with p_i. OF employs the Elliptic Curve Integrated Encryption Scheme (ECIES), which performs an ephemeral Elliptic Curve Diffie-Hellmann (ECDH) key exchange to derive a shared secret used to encrypt the report. According to [11], 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 retrieves 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.

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.

Figure 4: (a) Binary format of a location report   (b) Example of sent payload (images from [11],[10]).

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 [3]. 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 can identify various states in which AirTag can be; we will now quickly present all of them.

- *Not registered*: when the AirTag is brand new, has been reset, or has been removed from the FindMy network. It waits to be connected to while advertising itself every 33 ms.

- *Initialisation*: the AirTag is registered to an Apple ID and a public/private key pair is generated and shared between the AirTag and the connected iOS device.

- *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, the AirTag uses an NFC antenna to allow anyone who finds an AirTag to potentially identify the owner, even if they have an Android device. The tag can only be read when the AirTag is powered by a battery and it contains a URL to uniquely identify the AirTag, depending on its current state. There are some parameters that are attached to the URL, used to identify the device; we will briefly present them. 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.

4.3.1   Vulnerabilities

4.3.1.1   Side-channel attacks

The Nordic nRF52832 has the function Access Port Protection [24] that is used to disable access to the Debug Port through SWD and prevent reading out the internal memory; however, according to [23], 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
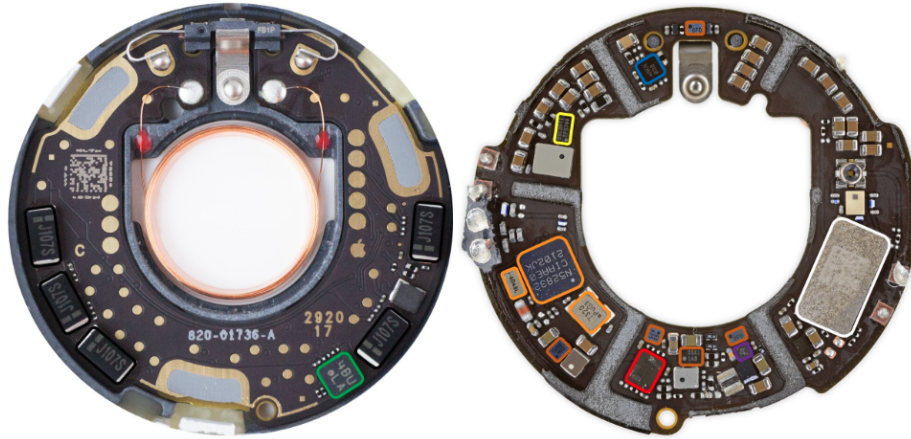
```
🟠 Nordic nRF52832 SoC with BLE and NFC, plus 32MHz and 32.768kHz crystals
⚪ Apple U1 UWB Transceiver
🔴 GigaDevice GD25LE32D 32Mbit NOR flash
🟢 Bosch BMA280 accelerometer
🔵 Maxim MAX98357AEWL audio amplifier
🟡 TI TPS62746 DC-DC buck converter
🟣 TI TLV9001IDPWR opamp
⚫ 100uF Electrolytic Capacitors (5x)
🟤 Unknown. Unable to decode markings
```

Figure 5: PCB overview (image from [3]).

phone or run (on the AirTag) a custom firmware since Apple does not check the signature of it (the firmware).

4.3.1.2 Insecure Storage

The GD25LE32D 32Mbit NOR flash is not encrypted, as we can see in [19]; 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.

4.3.1.3 Replay attacks

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: 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.

14

4.3.2 Anti-stalking measurements

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.

Additionally, AirTags are designed to emit sound if they have been separated from their owner for an extended period, potentially alerting the victim to the presence of the tracking device. 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. 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 [18], 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. This means that the AirTag will function as normal without emitting sounds; thus, an attacker can easily modify an AirTag and be unknowingly placed in someone's possessions to track a target's location without them being audibly notified of its presence.

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 [15] and, as we could expect, it seems that the AirTag doesn't work quite when in motion, as example on a moving cat.

- Child Safety: similarly to pets, AirTags can offer an additional layer of security for keeping track of children in crowded or unfamiliar places. By attaching an AirTag to a child's backpack or clothing, parents can monitor their child's whereabouts and receive alerts if they stray too far.

- Vehicle Tracking: AirTags can also be used to track vehicles, such as bicycles, motorcycles or cars in the same way as the two above.

- People with Dementia Tracking: people with Alzheimer's or another form of dementia can lose their ability to recognize familiar places, so it's not uncommon for them to wander off and get lost and confused; in this case, we can use AirTags to be sure about where they are.

4.5   Mods

After some Internet research, the author discovered that the AirTag has been modified in certain ways. For instance, in [4] 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 6 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. Section 1 offered a broad overview of the themes to be addressed,
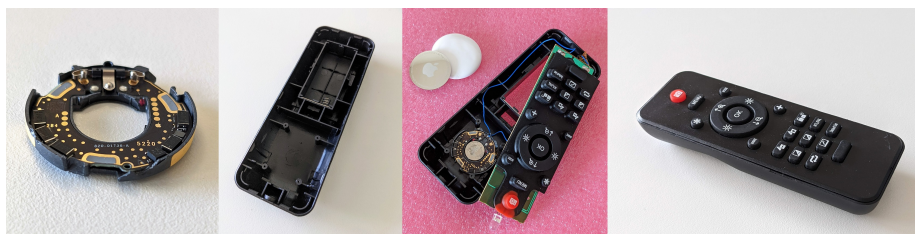
Figure 6: AirTag inside a remote control (images from [3]).

setting the stage for a deeper investigation. Section 2 delved into UWB technology, offering not only a general introduction but also a detailed analysis of its security implications, particularly in the context of Apple's implementation.

Progressing to Section 3, the focus shifted to the FindMy network. Here, the discussion began with an overview, followed by a practical example to illustrate its operation. Subsequently, an examination of FindMy's security measures was conducted, shedding light on the intricacies of its encryption protocols.

Section 4 centered on AirTag, starting with an overview before analyzing its architectural components, encompassing both software and hardware aspects. This was followed by an in-depth security analysis, uncovering vulnerabilities inherent in these devices that could potentially be exploited by malicious entities. Despite their cost-effectiveness and utility, it was evident that improvements in security measures, such as the introduction of authentication protocols during key exchange, were necessary to fortify their defenses against replay attacks, as discussed in 4.3. Lastly, the paper briefly report practical applications of these technologies, including an example where modifications were applied to adapt them to alternative contexts.

References

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

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

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

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

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

[6] 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.

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

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

[9] 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.

[10] 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.

[11] 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.

[12] 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..

[13] 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.

[14] 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.

[15] 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/.

[16] 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/.

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

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

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

[20] 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/.

[21] Renesas. *Defend Your Vehicle Against Relay Attack: Defense Technology Against Latest Automotive Theft*. s.d. URL: https://www.renesas.com/us/en/document/whp/defend-your-vehicle-against-relay-attack-defense-technology-against-latest-automotive-theft.

[22] 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/.

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

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