Apple's AirTag: A Security Vulnerability Discussion and Guide to Personal Safety

Tyme Hopkins and Nathan Hutchins, Ph.D
The University of Tulsa

Abstract

With over 55 million units sold in its first year, Apple's AirTag has become a popular device for locating lost items. However, its rapid adoption has also sparked concerns about potential misuse. Ever since the release of AirTags, local law enforcement saw an increasing trend in stalking and domestic violence cases involving AirTags. This paper delves into the security vulnerabilities and provides ways users can protect themselves from the potential misuse of AirTags. We examine how AirTags could be used for stalking, unauthorized tracking, and even theft. By outlining these vulnerabilities, we aim to raise awareness and potentially guide future security improvements for Apple's AirTag.

Keywords

AirTag, Find My, AirGuard, Tracker Detect, undergraduate student poster

Introduction

The rise of consumer tracking devices, like Apple's AirTag and its competitors, has revolutionized the way we keep tabs on our belongings. These small, easily concealable gadgets offer a convenient solution for locating misplaced keys, wallets, or even luggage. However, their ability to track a target's location in real-time has introduced a concerning dilemma to this technological advancement.

Reports of these devices being misused for malicious purposes, particularly in stalking and domestic violence situations, have become increasingly common. The very features designed for item recovery – long battery life, discreet size, and anonymous tracking – can be exploited by individuals with harmful intentions. This raises a critical question: how can we ensure the safety and privacy of individuals while still allowing consumers to benefit from the convenience of these tracking devices?

This paper discusses the growing challenge of unauthorized tracking with a specific focus on empowering consumers with the current and most up to date methods in protecting themselves from malicious threats posed using Apple AirTags. We'll analyze the security vulnerabilities inherent in these devices and explore the specific threats they pose. Our primary objective is to equip consumers with the tools and knowledge they need to effectively locate and disable AirTags being used for malicious purposes. By providing practical solutions and fostering collaboration, we aim to bridge the gap between technological innovation and public safety.

Background

Apple's AirTag is a tracking device designed specifically for tracking users personal belongings. AirTags work by using Bluetooth Low Energy (BLE) and Ultra-wideband (UWB) technology. The BLE embedded within the AirTag is used for close range communication with Apple devices within the Apple network. This "Apple network" is commonly known and referred to as the Find My network and is available via the Find My app on Apple devices. The idea behind the Apple network is very similar to crowd sourcing. A lost AirTag will transmit BLE signals which will then be received by nearby Apple devices with a network connection (iPhones, iPads, Macs, etc.). Once a user's lost AirTag signal is received by one of these devices, the Find My network, which works by using iCloud, will locate the device the AirTag is associated with and notify the user their personal belonging(s) has been found.

The UWB technology is utilized when users are searching for their AirTag in close proximities. Apple's Find My app has a built-in user interface that displays the nearby distance of your AirTag and works best between 30-40 feet from the device. It is important to note that this software feature is called precision finding and will only work for users with iPhone 11's and up.

In addition to the helpful precision finding technology, Apple also included a chirp feature that can also be triggered from the Find My app. This feature is very useful when one may be right by their AirTag but are still having difficulty finding the device. The chirp feature is connected via BLE and has various chirp modes for various purposes, but mainly location detection. Another benefit this feature has to offer is it works for all iPhone, iPad, and iPod Touch users running iOS or iPadOS 14.5 or higher. In summary, iPhone's 4S and higher use BLE technology, but only iPhone's 11 and higher use UWB technology, however Apple's AirTag is only compatible with devices running iOS or iPadOS 14.5 or higher.

Apple is known for their clean, modern, and sleek designs and that is a very apparent characteristic of the AirTag. Weighing in at just 11 grams and measuring 1.26 inches in diameter by 0.31 inches in height, the AirTag is a very small and versatile device. It is safe to say the sleek versatility of this device is one of the main reasons Apple has had so much success with this product. In addition to the AirTag's smooth design, it can also last over a year in battery life with a standard battery. The vast majority of AirTags will be used in many settings and not always the cleanest and electronically friendly either. As far as durability the AirTag is rated IP67 making the device water resistant within 1 meter of water for up to 30 minutes [1]. Additionally, the device contains extra support from its hard plastic and stainless-steel casing. From a hardware perspective, Apple's AirTag seem to be a very rugged and trustworthy tracking device.

Security Vulnerabilities

One of the main security concerns Apple's AirTag poses is the potential for stalking and domestic violence cases. Apple released the AirTag in April of 2021 and just within a year later, stalking cases involving AirTags skyrocketed. In April of 2022, there were 150 police reports filed in the US for stalking cases involving AirTags [2]. Hardware reverse engineering

techniques such as AirTag speaker removal, cloning, and NFC URL manipulation make AirTags much more of a threat when it comes to unwanted tracking.

Apple's AirTag produces a chirp sound whenever it is no longer in the presence of its owner and moving away for someone to hear and find. Removing the AirTag speaker is a simple yet significant reverse engineering tactic. AirTags have 6 various chirp modes and 5 of those are related to device location detection [5]. If the speaker is removed the only way of being alerted if there is an AirTag nearby is by the iPhone tracker notifications and possibly, if close enough, the NFC URL notification. The speaker removal process is very easy process and takes less than a minute to complete. Once an AirTag loses its chirp capability it is completely up to the user's software settings as to if they will be protected or not.

NFC URL manipulation is another way to create a malicious AirTag. In the event the NFC URL has been tampered with the victim could potentially be alerted there is an AirTag nearby and the NFC URL could be malicious. Clicking on unknown URL's can potentially give hackers the power to identify user credentials, therefore, the victim's passwords, personal data, and full access to their account can be accessed. Though more complex of an attack than removing a speaker it is still relatively simple to accomplish by changing the firmware and re-pushing this modification to an AirTag. The important component to remember with this attack is the AirTag isn't necessarily doing any "unwanted" tracking. The idea behind this attack is for the user to find the AirTag and be exploited via the NFC URL.

A more complex and much more effective attack for unwanted tracking is by cloning an AirTag. Cloning an AirTag questions every bit of the device's security integrity. AirTags are tied to the iCloud account of the user who set the AirTag up through their Find My app. Cloning an AirTag involves extracting the firmware and using another device to push the firmware to and connecting to iCloud. Cloning allows for a few things to happen. First, you can steal an AirTag and reset it with a new serial number. Second, SPI-Flash nor U1 are involved in pairing so you now can bypass lost mode functionalities. Lastly, one of the most concerning aspects involved in cloning an AirTag is that you can modify the nRF chip code to eliminate the AirTag notifications users receive when an AirTag has been traveling with them [6]. In summary, cloning an AirTag gives you almost full customization over the device and allows for the AirTag to be completely stealth, therefore making it a much more dangerous threat towards potential stalking cases.

Personal Safety and Security Considerations with Apple's AirTag

The surge in popularity of Apple's AirTag has coincided with a rise in stalking cases, highlighting various security vulnerabilities as previously discussed. This section explores the prevention of specific threats posed by AirTags, including speaker removal, NFC URL manipulation, and cloning. We will provide practical advice for users to mitigate these risks and protect their personal safety. While it's impossible to guarantee complete protection from all threats, implementing these measures can significantly reduce vulnerability.

As simple as it may sound the only way to protect and be aware of speaker removal from an AirTag is simply by removing the stainless-steel cover that holds the battery in place and examining the surrounding edge of the plastic covering. If it looks scratched or like it has been tampered with then the next test would be to connect to the AirTag and try and play the sound

through the Find My app. If you don't hear anything and the device is still within range of your Apple device pinging the AirTag, then the speaker has most likely been tampered with and you should consider contacting your local law enforcement authorities.

NFC URL manipulation may seem more difficult to protect against, but it is also very simple. Whenever the NFC URL is triggered, if the Apple site that should pull up has been changed to a malicious link, it will read the URL title when the NFC notification populates onto your Apple or Android device. This may seem like a harmless attack due to the ease of protecting against this threat, but often times many people don't read or think twice and click whatever link is in front of them. One key piece of general security advice to mention here is that you should always double check and be aware of your surrounding and the information you are trying to access.

Unfortunately, protecting against AirTag clones is much more difficult as they are very stealth, which is in fact the idea coming from a malicious perspective. Though it is very tough to protect completely against this attack, there are ways to help prevent unwanted tracking. The best way is to download the app AirGuard. AirGuard is a great tool because it will pick up any tracking device via any signal being populated, which means, yes it will pick up the AirTag clones. AirGuard is also very responsive and works for both iOS and Android devices. It is safe to use and was developed by researchers at the Technical University of Darmstadt. The same developers of this app also wrote an in-depth research paper on the full security vulnerabilities that AirTag's pose and the technical breakdown of the attacks as well as the best ways to protect yourself [3]. The second layer of protection, which unfortunately doesn't protect against AirTag cloning completely is to enable device tracking notifications via Apple system settings and the Find My app [7]. These Apple settings unfortunately only protect against registered AirTags and not cloned AirTags or other unwanted nearby tracking devices, which is just one more reason everyone should look towards using AirGuard.

Conclusion

Apple's AirTag has introduced a complex interplay between convenience and security. While designed for benign purposes, the device's vulnerabilities have facilitated its misuse for stalking and surveillance. Techniques like cloning and firmware manipulation emphasize the need for heightened security measures. To mitigate these risks, individuals must remain vigilant, employing a combination of technological safeguards and personal awareness. As technology evolves, so too must our approach to protecting personal privacy in an increasingly interconnected world.

References

[1] K. McElhearn, “How Tough are AirTags? We Froze, Washed and Dried, Ran Over, and Put Them in the Hot Sun,” *The Mac Security Blog*, May 12, 2021. [Online]. Available: https://www.intego.com/mac-security-blog/how-tough-are-airtags-we-froze-washed-and-dried-ran-over-and-put-them-in-the-hot-sun/ [Accessed June 27, 2024].

[2] A. Belanger, “Apple AirTags stalking led to ruin and murders, lawsuit says,” *ars Technica*, October 12, 2023. [Online]. Available: https://arstechnica.com/tech-policy/2023/10/apple-airtags-triggered-explosion-of-stalking-reports-nationwide-lawsuit-says/#:~:tex [Accessed June 27, 2024].

[3] T. Roth, F. Freyer, M. Hollick and J. Classen, "AirTag of the Clones: Shenanigans with Liberated Item Finders," 2022 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, USA, 2022, pp. 301-311, doi: 10.1109/SPW54247.2022.9833881.

[4] J. Clover, “Apple Enhancing AirTags Anti-Stalking Measures With Android App and Shorter Sound Intervals,” *MacRumors*, June 3, 2021. [Online]. Available: https://www.macrumors.com/2021/06/03/apple-airtags-anti-stalking-measures/ [Accessed July 2, 2024].

[5] Chaitanya, “Do AirTags Make Noise And How To Fix?,” *ElectronicsHub*, June 4, 2024. [Online]. Available: https://www.electronicshub.org/do-airtags-make-noise/#:~:text=Here%20is%20a%20breakdown%20of,when%20your%20locating%20the%20AirTag. [Accessed July 10, 2024].

[6] T. Roth, “Hacking the Apple AirTags,” *DEF CON 29*, DEF CON, 2021. [Online]. https://doi.org/10.5446/54241 [Accessed July 29, 2024].

[7] “What to do if you get an alert that an AirTag, set of AirPods, Find My network accessory, or compatible Bluetooth location-tracking device is with you,” *Apple Support*, [Online]. Available: https://support.apple.com/en-us/119874 [Accessed July 12, 2024].

Tyme Hopkins

Tyme Hopkins, an Electrical Engineering undergraduate at The University of Tulsa, demonstrates exceptional leadership within the department and across campus. As a transfer student peer mentor, student activities board member, and IEEE Vice President, Tyme fosters a welcoming and engaged environment. He has also led initiatives like high school student tours, departmental networking events, and resume and soldering workshops. Notably, Tyme organized an antenna seminar series featuring industry experts, showcasing his commitment to expanding educational opportunities for local STEM students.

Nathan Hutchins, Ph.D

Nathan is an engineer and educator currently serving as applied assistant professor of electrical and computer engineering at The University of Tulsa. Nathan attended The University of Tulsa for his B.S. in electrical engineering. After working as a civilian engineer for the U.S. Air Force, he came back to The University of Tulsa for his graduate education, researching autonomous systems, specifically human factors, and user acceptance of autonomous cars. After completing his Ph.D. in 2018, Nathan began teaching and research full time at The University of Tulsa where he is currently educating new engineers and researching autonomous systems, cyber-physical security, and rapid prototyping of RF circuits.