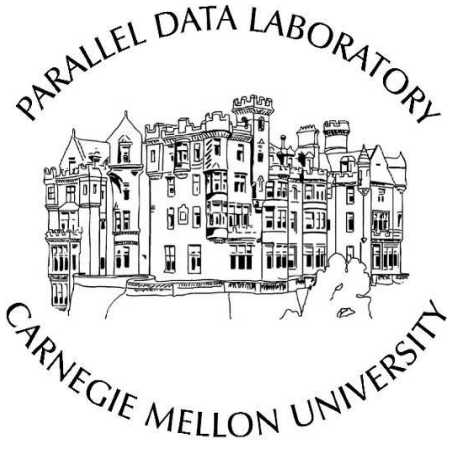

A Survey of Security Vulnerabilities in Bluetooth Low Energy Beacons

Hui Jun Tay, Jiaqi Tan and Priya Narasimhan

CMU-PDL-16-109
November 2016

Parallel Data Laboratory
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Abstract

There are currently 4 million Bluetooth Low Energy beacons, such as Apple's iBeacons™, deployed worldwide, with more being used in an increasingly wide variety of fields, from marketing to navigation. Yet, there is a lack of focus on the impact of security on beacon deployments. This report looks to capture an overview of current beacon deployments, the current vulnerabilities and risks present in using such platforms, and the security measures taken by vendors today.

Keywords: Bluetooth Low Energy, BLE, Security, iBeacon

1 Introduction

Beacon technology is one of the fastest growing technological industries in recent years. 2015 saw about 4 million beacon units deployed world-wide [26], with a predicted 60 million beacons to be shipped by 2019 [10]. Beacon technology sees increasing use in retail and industry for tasks such as proximity-based advertising, with potential applications in a wide variety of fields ranging from assistive technologies to proximity-based authentication. With this rapid adoption of Beacon technology comes an increasing awareness of the inherent vulnerabilities in its current deployment, and a need for addressing the potential security issues that could arise as the usage of Beacon technology becomes more ubiquitous.

This report consolidates current investigations into the vulnerabilities of the iBeacon™[1] protocol and examines them alongside existing use cases that employ such technologies. Focus is placed on the iBeacon protocol as it is one of the most widely supported of the existing Beacon protocols [26]. Examples were chosen based on scale, publicity and potential consequences. Section 1 provides an overview of the iBeacon protocol. Section 2 highlights the existing vulnerabilities in iBeacons with reference to real-world examples which showcase the exploitation and consequences of the vulnerability. Section 3 situates these vulnerabilities in the context of existing real-world use cases that utilize the iBeacon protocol, while highlighting the potential consequences the vulnerability can have on the use case. Section 4 compares the most common iBeacon platforms in use and their current defenses against these vulnerabilities. Section 5 concludes the report. In doing so, this report aims to provide a clear view of the current state of iBeacon security and the shortcomings that need to be addressed if the technology is to fulfill its potential moving forward into widespread use.

2 iBeacon Overview

The iBeacon protocol is essentially a means of associating a specific, abstract location with a particular Bluetooth signal. The technology employs Bluetooth Low Energy to constantly broadcast an advertising packet containing a UUID (Universally Unique Identifier) used to identify a particular beacon. The iBeacon protocol also includes a field that allows the calculation of relative distance from the beacon [18]. Applications that match the beacon's UUID registered in their database can then perform specific tasks based on the knowledge that the beacon is nearby. In most applications, this is used to provide the concept of region-monitoring [7], where certain functions are dependent on the users location within the 'region' created by a beacon or a network of beacons. By mapping a set of beacons to a predetermined set of regions, applications will know the user's actual location without the use of GPS.

3 Types of Vulnerabilities

3.1 Spoofing

Spoofing is the most widely-known vulnerability. Since a beacon broadcasts its UUID publicly, any third-party may utilize a sniffing tool or similar tool to capture a specific beacon's UUID. This allows them to impersonate that beacon anywhere they desire, breaking any assumptions made by applications that depend on the beacon to prove that a user actually visited a particular location. On the reverse side, knowing the UUID allows third-party applications to take advantage of an existing beacon network to leverage their own services, essentially 'piggybacking' on another party's infrastructure without any investment [30].

[1] iBeacon™ is a trademark of Apple Inc., registered in the U.S. and other countries.

3.2 Denial of Service

Denial of Service in the context of iBeacons can be broken into two categories: battery drain attacks and crashing the Bluetooth stack. In either case, the end-goal is to render the device non-operational. Since most beacons are stand-alone devices, they possess a configuration layer in addition to the advertising layer that a vendor-specific application uses to configure the beacon. Denial of service attacks target this layer to either drain the battery life of the device through constant activity, or to crash the beacon itself. Battery drain attacks are of particular relevance in deployments that use lightweight beacons with small battery capacities. Identifying dead beacons and performing replacements has been noted to be a particular hassle by current adopters of the technology [15].

3.3 Hijacking

Hijacking involves an unauthorized third-party gaining access to the configuration layer of the iBeacon. This allows them to control the operational settings of the beacon, including the UUID. Hijacking allows an attacker to perform any of the two previous attacks, with the added potential to 'lock out' the owner of a particular beacon by changing the authentication data. We conjecture that attackers could use this to ransom an iBeacon network in the manner of a ransomware attack [8], charging money for the original owners to gain access to an already-deployed iBeacon network.

The table below summarizes the three vulnerabilities and cites a specific case study where such a vulnerability manifested or was exploited on an existing beacon platform:

Potential Vulnerability	**Examples**	**Real-World Example**
Spoofing	Copying an existing iBeacon UUID and creating a replica Using an existing iBeacon UUID to take advantage of an existing iBeacon infrastructure	iBeacon UUID spoofing used to win scavenger hunt without being physically present [14]
Denial of Service	Battery Drain Attacks on the iBeacon device Crashing iBeacon device with packet pings Bugs in the protocol implementation resulting in undetected beacons	Apply iOS 7.1 bug causes issues in finding/ranging iBeacons [25]
Hijacking	Changing the UUID and configurations on iBeacon device by unauthorized third-parties	Reverse engineering app API to modify Estimote using EstimoteEditor [17], a third-party application that was able to modify any Estimote beacon even if not the owner [13]

4 Consequences in Real-World Deployment

This report chooses to classify existing iBeacon deployments into one of four fields: targeted notifications, tracking/metrics, navigation, and authentication. While notifications and metrics are already widely adopted in areas like retail and sports [27], navigation and authentication are still relatively uncommon [22].

Correspondingly, navigation and authentication are also fields with the most potentially serious security consequences.

4.1 Targeted notifications

Targeted notifications refers to the use of beacons to provide location-awareness in applications that look to push advertisements, offers or information. Common uses of notifications are in retail for advertising and product sale information, and in tours of places like museums, where information displays can be triggered by proximity to an exhibit [22].

4.2 Tracking and Metrics

Tracking and metrics encompasses location-based rewards and loyalty tracking. Applications use beacons to collect data on a users behavior relative to a particular location. This extends to rewarding repeat customers that return to the same store, or providing discounts to fans who show up at the stadium itself for a game.

4.3 Navigation

Navigation applications use beacons to map out an area in places where GPS might lose accuracy. Indoor navigation applications in places like hotels and airports use beacons to identify the user's current location and provide directions to the room or flight. A similar method is applied to assistive technologies, allowing visually-impaired persons to navigate indoors by using beacons to identify obstacles and visual landmarks.

4.4 Authentication

Authentication involves using beacons to provide an additional layer of identification through proximity to a physical location. Applications detecting a specific beacon can use the UUID to limit operations to a geo-fence – e.g., secure doors will open only when the user is nearby, certain sensitive services will only be accessible when inside a secure location like the user's home or the main store office.

The table below summarizes the different iBeacon applications alongside an example use case as well as the potential consequences each vulnerability might have on the application.

Application	Real-World Use Case	Potential consequences of vulnerability		
		Spoofing	**Denial of Service**	**Hijacking**
Location-Based rewards	MLB (Major League Baseball): MLB At Bat app incorporates iBeacons to provide location based advertisements and rewards [29]	Abuse of rewards	Service Loss, Customer dissatisfaction	Falsification of data, Lock-out
Loyalty Tracking	Adored: Start-up app that provides common platform for small businesses to provide location-based promotions and loyalty points, based in Manchester, England [24]	Abuse of loyalty points	Service Loss, Customer dissatisfaction	Falsification of data, Lock-out
Indoor Navigation	Nextome: European startup promoting iBeacon based indoor positioning and navigation system [6]	Misdirect users	Service Loss, Lost users	Location Swapping, Lock-out
Assistive Technology (Blind)	Wayfinder: iBeacon application that helps visually-impaired users to navigate the London transport network [16]	Misdirection, potentially malicious use	Service Loss, Blind-spots, safety failure	Misdirection (potentially malicious), Lock-out
Proximity-Based Advertising	ShopKick: Retail application offering deals and advertisements to encourage customer behavior [20]	Spam, Piggybacking	Loss of potential advertising	Falsification, Lock-out
Proximity-Based information (tours)	Museums[2]; Facebook: Context-based content delivery using the user's location [12]	Spam, Piggybacking	Content-provider Downtime, Customer dissatisfaction	Falsification , Lock-out
Proximity-triggered programs	Beecon: App that enables use of iBeacons for smart-home automation [19]	Inaccurate behavior, Unauthorized access	Loss of service, program failure	Falsification , Lock-out
Proximity-based authentication	Location-based One-Time-Passwords: Study in using iBeacons as an additional factor to create location-based OTPs [28]	Geo-fence invariant broken could lead to unauthorized access	Accessibility failure (downtime)	Falsification , Lock-out

5 Current iBeacon Defenses

Of the 7 beacons surveyed, only 2 have listed defenses against all three vulnerabilities on their platform. In many cases, the exact details of these security implementations were vague and obscure. This is possibly an attempt at security through obscurity for example, in the 4 platforms that employed a defense against

[2] http://blog.beaconstac.com/06/how-museums-can-use-beacons-to-enhance-visitor/

spoofing, 3 used a rotating UUID scheme to mask the real UUID from being publicly accessible. Estimote however, had an implementation that simply rotated through "3 UUID + Major + Minor combinations" using "table based lookups" [11]. Sniffing all combinations would still enable a spoofing attack, showing that implementation of a rotating UUID does not guarantee security, especially if the implementation is incomplete.

Beacon Vendor	**Spoofing**	**DDoS**	**Hijacking**
Estimote [23]	"Secure UUID" - Rotating UUID w/ limited token scope	-	Cloud-based token authentication
Gimbal [5]	Private Mode with Rotating UUID	Time-limited configuration window	Time-limited configuration window
BlueCat [1]	"Secure Mode" periodically changed encrypted UUID	-	API token authentication
Konkat.IO [2]	"Secure Shuffling" randomly rotating UUID (daily)	Black-list for brute-force attacks (non-connectable mode)	Secure Communications, Software Lock
Radius Networks [21]	-	Time-limited configuration window, Time-limited service with "auto-disconnect"	Time-limited configuration window, PIN-protected "Lock configuration"
Gelo [3]	-	Separate config/beacon mode	Two-factor authentication, passcode access
GemTot [4]	-	-	API token authentication

6 Conclusion

Beacons are an increasingly important technology today. However, while plenty of research exists regarding its application in a wide variety of fields, developers agree that security issues with the iBeacon protocol hamper its viability in the industry [9, 28]. Currently, iBeacons have yet to be the target of a malicious attack, likely due to its lack of ubiquity and usage outside of areas like advertising, where a security flaw has limited consequences. However, current trends suggest that the field is changing, with pushes to utilize iBeacons in areas with very real consequences for security failures. As the field continues to grow, it is essential that vendors catch up their security to match, before iBeacons grow popular enough to become a target.

References

[1] *Secure Mode and iBeacon + Secure Mode*, August 2015. http://support.bluecats.com/customer/portal/articles/ 1525982-secure-mode-and-ibeacon-secure-mode.

[2] *Common attacks and how Kontakt.io can protect you*, May 2016. http://gofor.kontakt.io/beacons-security/.

[3] *Gelo Developers*, May 2016. http://www.getgelo.com/developers/.

[4] *GemTot Beacon Specifications*, May 2016. https://passkit.com/gemtot-beacons-eddystone-ibeacon-altbeacon/.

[5] *Gimbal iBeacon Configuration*, May 2016. https://docs.gimbal.com/proximity\–overview.html\#beacon\–configuration.

[6] *Nextome*, May 2016. http://www.nextome.net/en/indoor-positioning-technology.php.

[7] *Region Monitoring and iBeacon*, March 2016. https://developer.apple.com/library/ios/ documentation/UserExperience/Conceptual/LocationAwarenessPG/RegionMonitoring/RegionMonitoring.html.

[8] *Trend Micro: Ransomware*, May 2016. http://www.trendmicro.com/vinfo/us/security/definition/ransomware.

[9] Nicholas Woodward Torin Zonfrelli A. Joseph Ruffa, Amy Stevens. Assessing ibeacons as an assistive tool for blind people in denmark. Master's thesis, Worcester Polytechnic Institute, May 2015.

[10] ABIresearch. ibeacon/ble beacon shipments to break 60 million by 2019, July 2014. https://www.abiresearch.com/press/ ibeaconble-beacon-shipments-to-break-60-million-by/.

[11] Sandeep Mistry Alasdair Allan. Beware the hackable google beacons made by estimote, August 2015. http://makezine.com/2015/08/04/ beware-hackable-google-beacons-made-by-estimote/.

[12] Reed Albergotti. Facebook tests bluetooth beacons to feed users local content, January 2015. http://blogs.wsj.com/digits/2015/01/29/facebook-tests-bluetooth-beacons-to-feed-users-local-content/.

[13] Alasdair Allan and Sandeep Mistry. Reverse engineering the estimote, January 2014. http://makezine.com/2014/01/03/reverse-engineering-the-estimote/.

[14] Alasdair Allan and Sandeep Mistry. Hacking the ces scavenger hunt for a second time, January 2016. http://makezine.com/2016/01/07/ hacking-ces-scavenger-hunt-second-time/.

[15] Shelley Bernstein. The realities of installing ibeacon to scale, February 2015. https://www.brooklynmuseum.org/community/blogosphere/2015/02/04/ the-realities-of-installing-ibeacon-to-scale/.

[16] Katie Collins. Wayfinder app helps the blind navigate the tube, August 2014. http://www.wired.co.uk/news/archive/2014-08/12/wayfindr-app.

[17] Yoann Gini. Estimoteeditor, December 2014. https://github.com/ygini/EstimoteEditor.

[18] iBeaconInsider. What is ibeacon? a guide to beacons, May 2016. http://www.ibeacon.com/what-is-ibeacon-a-guide-to-beacons/.

[19] Ricardo Menezes. Beecon, May 2016. http://www.beaconsandwich.com/.

[20] Tim O'Brien. Smartphones deals turn store shoppers into buyers, December 2015. http://www.timesunion.com/tuplus-local/article/Smartphones-deals-turn-store-shoppers-into-buyers-6693260.php/#photo-9099553.

[21] Sean O'Donnell. How do i lock my beacon settings, December 2015. https://radiusnetworks.zendesk.com/hc/en-us/articles/ 202478670-How-do-I-lock-my-beacon-settings-.

[22] Vladimir Petrov. ibeacon use cases since inception, February 2015. http://bluesensenetworks.com/ibeacon-use-cases-since-inception/.

[23] Agnieszka Steczkiewicz. Are estimote beacons secure? how does secure uuid work?, March 2013. https://community.estimote.com/hc/en-us/articles/ 201371053-Are-Estimote-Beacons-secure-How-does-Secure-UUID-work-.

[24] Rebecca Strong. Adored banks $2.3m seed to help merchants with mobile loyalty, July 2015. http://bostinno.streetwise.co/2015/07/08/adored-funding-ibeacon-technology-for-customer-loyalty/.

[25] Doug Thompson. Apple ibeacon bugs complicate bluetooth le experience, November 2013. http://beekn.net/2013/11/ apple-ibeacon-bugs-complicate-bluetooth-le-experience.

[26] Unacast. The proxbook report q4 2015. Technical report, Proxbook, January 2016.

[27] Unacast. Proximity marketing in retail. Technical report, Proxbook, April 2016.

[28] Roland van Rijswijk-Deij. *Simple Location-Based One-time Passwords*. PhD thesis, Radboud University Nijmegen, 2010.

[29] Chris Velazco. Mlbs ibeacon experiment may signal a whole new ball game for location tracking, September 2013. http://techcrunch.com/2013/09/29/mlbs-ibeacon-experiment-may-signal-a-whole-new-ball-game-for-location-tracking/.

[30] Craig Gilchrist Wojtek Borowicz. ibeacon security: Understanding the risks, December 2014. http://blog.estimote.com/post/104765561910/ ibeacon-security-understanding-the-risks.