# Case Study: Impact of the Physical Web and BLE Beacons

Debasis Bhattacharya, JD, DBA
University of Hawaii
Maui College
debasisb@hawaii.edu

Mario Canul
University of Hawaii
Manoa
mcanul@hawaii.edu

Saxon Knight
University of Hawaii
Manoa
knight7@hawaii.edu

## Abstract

*The Physical Web is a project announced by Google's Chrome team that provides a framework to discover "smart" physical objects (e.g. vending machines, classroom, conference room, cafeteria, bus stop etc.) and interact with specific, contextual content without having to resort to downloading a specific app. A common app such as the open source and freely available Physical Web app on the Google Play Store or the BKON Browser on the Apple App Store, can access nearby beacons.*

*A current work-in-progress at the University of Maui College is developing a campus-wide prototype of beacon technology using the Eddystone-URL protocol and beacons from vendors such as Estimote, Radius Networks and BKON. The project is also incorporating security issues using the new and emerging Eddystone Ephemeral-ID (EID) protocol from Google.*

## 1. Introduction

A beacon is a low-cost hardware that transmits a short burst of data over a small distance using the Bluetooth Low Energy (BLE) protocol. This data contains basic text information that could include a URL and other relevant information. Any smartphone that supports the BLE protocol can pick up this data signal and present the information to the user. As a result of this interaction, a user can receive contextual information from beacons as they come within its proximity or range.

Beacons are emerging as a novel technology for several types of businesses who provide contextual information based on the proximity of the user and the prevalence of smart phones. This case study presents an implementation of beacons within the context of an educational institution. However, the context and basis for this case study can be extended to other industries outside the educational arena.

## 2. Beacons in History

Beacons have been used throughout history to signal to users about dangerous situations or locations, or send coded messages during time of war. Most of the early beacons relied on the combination of fire, light or sound to convey a specific, coded message from the sender to the recipient. Given the physical location of the beacon (for example, on a dangerous coastline) the signal from the beacon would provide contextual information to the recipient. This concept of sending short bursts information from a physical to a recipient, who is within transmission range, is the fundamental basis for the creation and proliferation of these new BLE beacons.

## 3. Background – RFID and IoT

The technology behind the proliferation of BLE beacons is based on a history of similar advances. Radio Frequency Identification Devices (RFID) have been around for decades to provide short data transmissions over short distances to RFID receivers. Retailers such as Wal-Mart have used RFID extensively to improve their inventory and checkout systems. Despite the prevalence of RFID devices, there have been concerns among security professionals about their security concerns and limitations [2, 8, 9]. Several papers and publications have addressed these security issues over time and found solutions [11, 12, 17]. Privacy issues regarding RFID transmitters and receptors have also been covered in the literature [19].

The Internet of Things (IoT) refers to appliances, objects and other things that are enabled by access to the Internet. These objects could range from televisions, refrigerators, microwaves and other household objects, to physical locations and large objects such as buildings, buses and other physical things. With the accessibility of these things to the Internet, there are concerns about security and privacy, just as in the case with RFID. Various references to the security literature provide some solutions and

URI: http://hdl.handle.net/10125/41676
ISBN: 978-0-9981331-0-2

mitigation efforts [6, 10, 18]. As Gartner [15] recommends, the base for objects that are classified under the IoT umbrella will swell to 20 billion in 2020! With this explosive growth in the things connected to the Internet, the impact of BLE beacons cannot be ignored, nor can their security and privacy issues be ignored or dismissed as unimportant.

## 4. Beacons and the Physical Web

Apple first introduced beacons in 2013 at the Apple Worldwide Developers Conference. Using the iBeacon protocol, Apple demonstrated beacons that transmitted a small unique id from a transmitter to a receiver, which could be an Apple iPhone. These simple devices provided a unique ID and a short text description from the beacon and alerted iPhone and other users with basic information when they were within range.

In response to the offering from Apple, Google released their open specification of the Eddystone BLE beacon protocol in July 2015. The entire specification is available at GitHub (see https://github.com/google/eddystone) and is freely available to developers and vendors. The early specification of Eddystone was similar to iBeacon and focused on smartphones that supported the Android OS.

Over time, Google upgraded their Eddystone BLE beacon protocol to include more than short text descriptions. With the introduction of the Eddystone-URL protocol, supporting beacons could transmit a URL that would be resolved by a receiver (such as a smartphone). As a result, the recipient could obtain more information about the contextual information transmitted by the beacon, as the URL could potentially provide more information and details.

## 5. Security and Privacy Issues

The initial beacon protocols (iBeacon and Eddystone) from Apple and Google did not focus on security and privacy issues and concerns [1]. The BLE protocol also did not consider security and privacy issues and the usage of BLE with insecure beacons, essentially opened up the implementation to exploits [16]. With the emerging popularity of BLE beacons with retailers, hospitals, stadiums, educational institutions and other businesses, there were specific instances of security and privacy that were becoming too glaring to ignore [3].

A key paper by Google [20] identified the security issues and concerns with the current Eddystone and iBeacon technology. The authors described the key issues and concerns and provided a new protocol called the Eddystone Ephemeral ID (EID) as a proposal solution [7, 13, 14].

The security issues and concerns identified by the authors from Google [20] includes but is not limited to the following:

1. Tracking of beacon locations – Since the unique IDs from beacons can be received by many commonly available smartphone applications, it is possible to track the unique location of beacons. These locations identifiers can track the historical location of beacons and record their current locations.
2. Forgery – Given that the beacon transmission is not secure, an adversary can transmit forged information over a beacon channel, thereby harming the reputation and integrity of the sender.
3. Showrooming – In addition to the risks of forgery, an adversary can send competitive information over a beacon that is meant for a business, thereby confusing and misleading consumers. This showrooming could potentially cause harm to the original business.

## 6. Case Study: Physical Web and BLE Beacons in an Educational Environment

Given the above issues and concerns with BLE beacons, it is conceivable that an implementation within an educational institution comes with risks and concerns. As a result, the proposed case study at the University of Hawaii Maui College (UHMC) demonstrates the use of BLE Beacons from various vendors such as Estimote [1], Radius Technologies and BKON. Currently, beacon vendors are in varying stages of support for the EID protocol. As this project progresses at UHMC, new vendors may provide enhanced support for this emerging protocol.

The use of Eddystone EID [20] allows for registered users to access specific beacons, assuming they are authorized to do so. If a user approaches a beacon that he/she is not authorized to access, the user does not see the beacon at all. As a result, the Ephemeral ID, based on registration of the beacon with a "global resolver", allows only registered users to access specific beacons. Users need access to the Internet to be able to resolve their access credentials.

The project at the UHMC allows for the following common scenarios:

1. A college cafeteria can provide all students with the latest information about menu specials and hours;
2. A college library and other locations can provide hours and other information to users, when they come in proximity of the door or entrance area;
3. Conference rooms and classrooms can provide a brief text information and a specific custom URL that provides updated information on classroom schedule and changes (if any);
4. Faculty members can affix beacons on their office or lab doors to provide students with the latest URL and information on their classes and other updates. This information is provided with the user approaches the beacon location;
5. Finally, sports facilities and other event locations at the university can provide updated information about events based on an updated URL to the users who are in close proximity of the beacon.

All these beacons are managed by a centralized web-based management system that monitors the information that is broadcasted by the beacons, as well the battery strength and other specifics about the beacon. This management of beacon information provides the Information Technology (IT) staff with a tool to detect failing beacons and to update the URL as needed to provide users with the latest information.

## 7. Conclusion

BLE beacons are an emerging technology and have recently been deployed in various physical locations such as educational institutions. The Physical Web is a collection of locations, objects and things that are marked with a BLE beacon that can provide users in close physical proximity with latest information and updates. Given that many users use their smartphones to navigate the physical world around us, this physical web of beacons can provide with contextual information as users move from one place to another.

## 8. References


[1] Are Estimote Beacons secure? How does Secure UUID work? url: https://community.estimote. com / hc / en - us / articles / 201371053 - Are - Estimote - Beacons - secure - How - does - Secure - UUID-work- (visited on 06/15/2016).

[2] Giuseppe Ateniese, Jan Camenisch, and Breno de Medeiros. “Untraceable RFID tags via insubvertible encryption”. In: Proceedings of the 12th ACM conference on Computer and communications security. ACM. 2005, pp. 92–101.

[3] Beacons Have Been Vulnerable For Too Long. It’s Time We Fixed It. url: http://kontakt.io/ blog/beacon-security/ (visited on 04/10/2016).

[4] Bluetooth SIG. Specification of the Bluetooth○R System. Version 4.2. 2014.

[5] Eddystone-EID. url: https : / / github . com / google / eddystone / eddystone - eid (visited on 06/15/2016).

[6] Federal Trade Commission staff. Internet of Things: Privacy & security in a connected world. 2015. url: https : / / www . ftc . gov / system / files / documents / reports / federal - trade - commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/ 150127iotrpt.pdf (visited on 06/15/2016).

[7] Philippe Golle et al. “Universal re-encryption for mixnets”. In: Topics in Cryptology–CT-RSA 2004. Springer, 2004, pp. 163–178.

[8] Ari Juels. “Minimalist cryptography for low-cost RFID tags”. In: Security in Communication Networks. Springer, 2004, pp. 149–164.

[9] Ari Juels and Ravikanth Pappu. “Squealing Euros: Privacy Protection in RFID-Enabled Banknotes”. In: Financial Cryptography: 7th International Conference, Revised Papers. Springer Berlin Heidelberg, 2003, pp. 103–121.

[10] MIT Auto-ID Center. url: http://autoidlabs.org/wordpress_website/ (visited on 06/15/2016).

[11] David Molnar, Andrea Soppera, and David Wagner. “A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags”. In: Selected Areas in Cryptography. Springer. 2005, pp. 276–290.

[12] David Molnar and David Wagner. “Privacy and security in library RFID: Issues, practices, and architectures”. In: Proceedings of the 11th ACM conference on Computer and communications security. ACM. 2004, pp. 210–219.

[13] Nearby Messages API for Android: Get Beacon Messages. url: https://developers.google. com/nearby/messages/android/get-beacon-messages (visited on 06/15/2016).

[14] Proximity Beacon API Overview. url: https://developers.google.com/beacons/proximity/ guides (visited on 06/15/2016).

[15] Janessa Rivera and Rob van der Meulen. Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020. 2013. url: http://www.gartner.com/newsroom/id/2636073 (visited on 06/15/2016).

[16] Mike Ryan. “Bluetooth: With Low Energy Comes Low Security.” In: WOOT. 2013.

[17] Sanjay E. Sarma, Stephen A. Weis, and Daniel W. Engels. “RFID systems and security and privacy implications”. In: Cryptographic Hardware and Embedded Systems-CHES 2002. Springer, 2002, pp. 454–469.

[18] The Hierarchy of IoT “Thing” Needs. url: http://techcrunch.com/2015/09/05/the-hierarchyof-iot-thing-needs (visited on 06/15/2016).

[19] Stephen A. Weis et al. “Security and privacy aspects of low-cost radio frequency identification systems”. In: Security in pervasive computing. Springer, 2004, pp. 201–212.

[20] Avinatan Hassidim et al. “Ephemeral Identifiers: Mitigating Tracking & Spoofing Threats BLE Beacons”. url: https://developers.google.com/beacons/eddystone-eid-preprint.pdf (visited on 06/15/2016)