Security and Privacy in Public IoT Spaces

Albert F Harris III, Hari Sundaram, and Robin Kravets
Department of Computer Science
University of Illinois at Urbana-Champaign
{aharris,hs1,rhk}@illinois.edu

***Abstract*—This paper presents Lamina, a system for providing security and privacy to users in a public IoT space. Public IoT spaces, such as an IoT-enable retail store, have the potential to provide rich, targeted information and services to users within the environment. However, to fully realize such potential, users must be willing to share certain data regarding their habits and preferences with the public IoT spaces. To encourage users to share such information, we present Lamina, a system that ensures the user's data will not be leaked to third parties. Lamina uses CryptoCoP-based encryption and a unique MAC address rotation mechanism to ensure that a user's privacy is maintained and their data is protected while still allowing the public IoT space to collect sufficient information to effectively provide targeted services.**

I. Introduction

The progression of wireless communication into lower power, smaller form factor devices has heralded the age of the Internet of Things (IoT). Predictions show the integration of IoT devices into all facets of our public and private lives. It is not hard to imagine an IoT-enabled home that allows a user to interact with their personal environment or an IoT-enhanced store that advertises available products, enhanced with targeted offers to nearby or frequent shoppers. However, there are many dangers inherent in the use of IoT. Dealing with these dangers are particularly challenging in public spaces where users interact with IoT infrastructures not under their control.

Such scenarios bring visions of the stores learning too much about a user, as well as third party attackers injecting fake or malicious product advertisements into the environment and tracking the movements and behavior of the users. Privacy leaks originate from the user's devices themselves. If the device uses a constant WiFi or Bluetooth Low Energy (BLE) MAC address, it is essentially advertising to the world who it is and where it has been. While this hole can be plugged by randomly rotating the BLE MAC address, such an approach also hides the user from the store, eliminating any chance of getting recommendations or discounts.

Further problems relate to security issues. Any mechanisms that intentionally allow a store to track a user may inadvertently leak personal information to snooping attackers. Additionally, an attacker can insert false advertisements into the system, confusing the user and potentially hurting the profit of the business. Finally, a store may want to limit access to some IoT information based on location or registration of users, essentially allowing the store to push special sales to only targeted users.

Current solutions for securely transmitting data in IoT environments have relied on asymmetric cryptographic techniques such as public key cryptography (TLS, SSL, HTTPS). Although these traditional cryptographic solutions would prevent the above security concerns, such solutions are simply too resource intensive to function on simple BLE-based devices. Additionally, BLE typically provides no reliability and message loss is common. This fact, combined with the very small packet size (31 bytes) makes such traditional mechanisms completely impossible in practice.

These security solutions also rely on the use of a known MAC address during all interactions in a single public IoT space, which would lead to privacy leaks and user identification. Essentially, to ensure data could be encrypted, users would have to expose enough information to be effectively trackable by third parties. Two potential problems are an attacker "shadowing" a user through the public space to inject false user interactions or neighboring public spaces snooping on users in regions where communication coverage extends beyond a particular store's walls. However, if the user anonymizes too strongly, public IoT spaces can only provide limited services to users. For example, if the retail space can identify nothing about a user's spending habits, then it becomes impossible to offer targeted deals. Thus, a privacy and security system that aims to facilitate such potential advantages of an IoT system must allow enough information to be exposed to the public IoT space to enable some identification to be performed while protecting the users from third party information leakage.

In response to these challenges, we present Lamina, an IoT system that maintains secure communications while also supporting user-defined privacy levels. Lamina uses a cloud service, accessed through the use of 4G or cellular technology, to register with a public IoT space prior to interacting with it. In our first generation of Lamina, WiFi is not used for registration since the use of WiFi would leak user information much in the same way a static BLE address does, breaking the privacy model. During registration, the user and the IoT space exchange shared secrets. These secrets are then used to build AES key chains for use in encrypting each transmitted packet. Additionally, the shared secrets are used to alter the MAC address for each transmission, thus making it impossible for a third party to shadow or track a user's transmissions through the public space. Then, while within the public space, the user device utilizes an encryption algorithm to ensure transmitted data is secure. While changing MAC addresses in BLE is

inherently part of the protocol, changing WiFi MAC addresses is more complex and will require changes to the base station to maintain associations. We will explore the integration of WiFi into the Lamina architecture in future work.

The rest of this paper is structured as follows. Section II describes public IoT spaces. Bluetooth Low Energy (BLE) is introduced as the primary IoT communication protocol and security and privacy concerns in the IoT environment are outlined. Section III presents the architecture of the Lamina system. Section IV presents an analysis of impacts of the Lamina system on users and on public IoT spaces. Finally, Section V presents some conclusions and future directions.

II. IoT in the Wild

IoT has emerged as the *de facto* term for interacting with wireless devices in any environment. However, the solutions needed for different environments have different requirements and challenges. While IoT in the home focuses on management of a user's personal devices, IoT in public spaces requires secure and privacy preserving mechanisms to enable the user to interact with and exchange data with devices from other people and organizations. On one side, IoT-enabled retail spaces, such as department stores and supermarkets, must support secure and authenticated communication from the store to the user that puts limited resource burden on the user's low power, low computation devices. On the other side, these same spaces must provide privacy-preserving communication between the user and the store that enables the user to control how much personal information to expose.

Although the vision of such smart spaces has been around for many years, there was no consensus on what wireless communication technology would bring that vision to light. The problems stemmed from the fact that WiFi is too expensive in terms of energy, IEEE 802.15.4 (ZigBee) is not available on commodity user devices, Bluetooth Classic is too complex, RFID requires expensive readers, and near-field communication is too limiting in range. The introduction of Bluetooth Low Energy (BLE) filled a niche for systems that required low-power, infrequent, and low bandwidth communication with the current generation of smartphones. However, with the expectation of low power and small form factor comes the challenge of achieving the security and privacy goals using unreliable, low bandwidth wireless channels and limited processing power and storage.

A. Instrumenting Public Spaces with BLE

As the leading communication technology for commodity IoT devices, there are numerous inexpensive BLE tags and development boards available for outfitting objects throughout a public space (*e.g.*, Nordic Semiconductor nRF51822 BLE Smart Beacon [1] (see Figure 1)). Such objects can be individual items with IoT tags, such as the Nordic Smart Beacons, or they could be Internet connected devices with BLE capabilities, such as Nordic Semiconductor nRF51 dongles, that can be used to aggregate data from multiple objects in the space and provide specialized information over a low-power radio for users in the space.

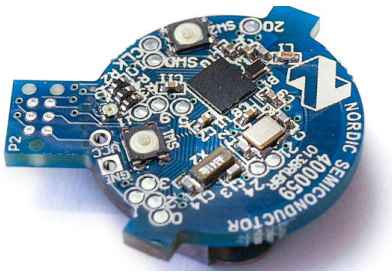

Fig. 1. nRF51822 Smart Beacon: Commodity BLE-based Tags for IoT Applications

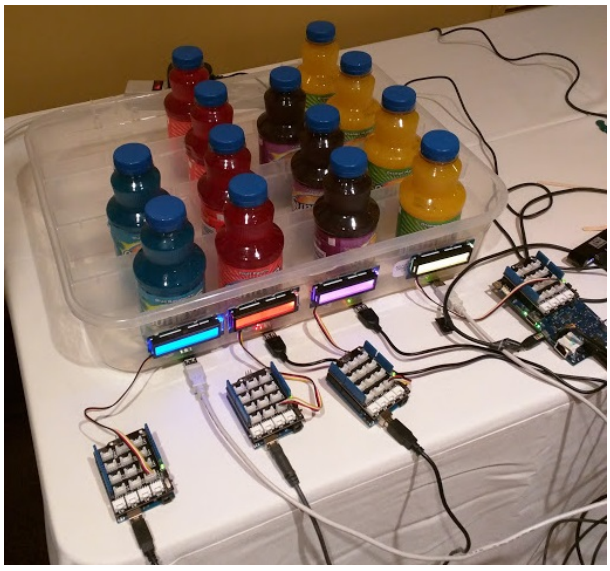

Fig. 2. Smart LaBLEs: IoT Hubs Capable of Aggregating Messages for IoT Tags and Broadcasting Aggregate Messages to Scanning Devices

For BLE-tagged objects, a grocery store may have each shelved products configured to advertise product information as a URL [2] or directly in the BLE packet as price and nutritional information. To prevent the overload of product information at the user's devices, Smart LaBLEs (see Figure 2) aggregate nearby product data regarding products, visually display relevant highlights of that data as well as send enhanced product information, coupons and other deals over BLE to the user [3]. However, the focus of the Smart LaBLE system was to automatically manage products, with no consideration for authentication or use management. To enhance Smart LaBLEs with the ability to send targeted or localized coupons and deals, a full security and privacy solution must be introduced in an energy efficient manner.

For users willing to expose their location and some level of personal information, BLE can be enabled on their smartphones or other BLE-enabled devices and can be used to interact with the public IoT space to access tailored recommendations and services [4]. Additionally, users frequently carry

Fig. 3. User Devices and Tags: Smartphone, Smartwatch, Eddystone Tags

one or more devices that can scan for BLE objects in the environment, even if they are not participating in the public IoT space (*e.g.*, smartphones and smartwatches, see Figure 3). While these user devices typically have more resources than embedded devices, in terms of computation ability, greater storage, and multiple communication options, they are still energy constrained and the public IoT system must be careful not to over-strain their batteries and processors by causing the devices to decode unnecessary messages.

B. BLE Services and Limitations

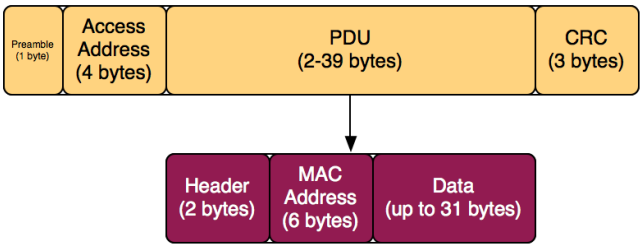

Fig. 4. BLE Advertising Packet Format

BLE was designed to reduce the high discovery and pairing energy cost and delay of classic Bluetooth. This is accomplished in part through the use of *passive scanning mode* in which a device, or "tag," sends an advertising message once every *advertising period* or *beacon interval*. Advertising messages are short messages that can be used to transmit a payload to all surrounding BLE scanning devices. The BLE advertising message contains a payload that includes a short header, a MAC address, and up to 31 B of data (see Figure 4).

The advertising period is adjustable and can be used to trade-off responsiveness for energy and channel congestion. Essentially, the shorter the advertising period, the more frequently each tag advertises its information, and thus the shorter the discovery time. However, shorter advertising periods also lead to increased energy consumption at each tag and increased channel congestion (due to the increased number of transmissions in a given time period). Typical advertising periods are between 100 ms and 1 s.

To further alleviate contention, BLE divides its frequency space in the 2.4 GHz band into 40 channels (see Figure 5). While most of the channels are dedicated to *connected mode* communication, BLE specifically reserves three orthogonal channels (channels 37, 38, and 39) for use in passive and active scanning modes. Additionally, these channels are between the typical bands used by WiFi, further reducing contention for BLE advertising messages and coexisting with WiFi more effectively. Tags transmit the same advertising message on each of the three advertising channels and then wait an advertising period. Scanning devices simply cycle through the advertising channels listening for advertising messages. Scanning devices, upon hearing an advertising message, can either enter active mode, where a handshake is performed to receive an additional 31 B of data, enter connected mode for extended data reception, or continue scanning if the 31 B of data in the initial advertising message is sufficient. In this paper, we focus on passive scanning, since in public spaces with an expectation of high density, passive scanning most efficiently uses the channel.

To reduce the energy consumption of BLE to a greater degree, the MAC protocol is very simple. All devices simply transmit messages without the use of carrier sensing. Tags randomly add up to 10 ms of jitter to every advertising period to help alleviate collisions. To save energy, all tags duty cycle, turning off when they are not in an advertising period.

While the design of BLE is certainly aimed at energy efficiency, the result is a low bandwidth channel of small unreliable packets. Although compensating for these limitations in the context of discovery can be handled through longer waiting times or additional information in the advertising messages, most security solutions break under these conditions.

C. Encryption in Public IoT Spaces

To reduce energy consumption and enable operation on small devices, IoT communications over BLE are typically not encrypted. However, given the personal nature of data that is collected and transmitted by user devices, as well as the information related to shopping habits that can be transmitted by retail stores, some level of data protection is desirable. While asymmetric encryption is intuitively a good fit for IoT [4], traditional asymmetric encryption is not suitable for use over a BLE channel for a number of reasons.

The first challenge is message size. Key exchange protocols, such as TLS or SSL, require large protocol messages, frequently up to 16 KB [5]. Furthermore, all of these large messages must be reliably transmitted for the encryption protocol to function as expected. Although not all encryption protocols have such large messages, even the ones with the

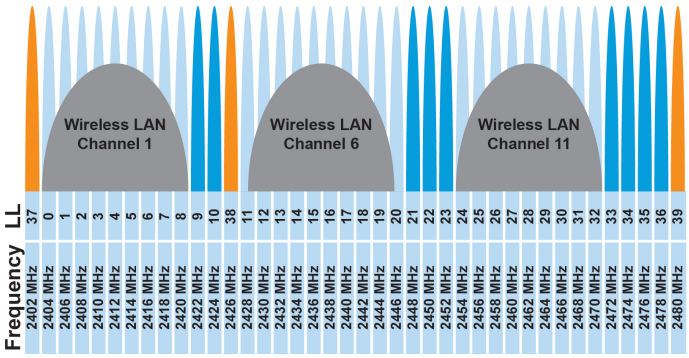

Fig. 5. BLE Spectrum Usage

smallest requirements use 276 B messages. This is at best problematic in a BLE environment that can experience high loss, lacks a reliable transmission stream, and has a maximum message sizes on the order of 31 B.

The next challenge stems from the fact that asymmetric encryption protocols, and even most symmetric encryption protocols, assume a reliable channel. For example, many rely on block chaining (*e.g.*, the Cipher Block Chaining (CBC) mode or the Cipher Feed Back (CFB) mode [6]). Such protocols link the output of previous blocks with the current blocks being encrypted. Therefore, if the receiver does not successfully receive the entire chain of messages, synchronization is lost and successful decryption cannot be accomplished. Again, such reliability does not exist in the BLE environment.

As with many mobile and embedded systems, BLE devices are typically energy constrained. Therefore, computationally complex algorithms simply require far too much energy. For example, a single key exchange for a very-small-key protocol called ECDH-ECDSA required 6,000 times as much energy as encrypting a block using symmetric operations [7]. Thus, the computational overhead of key exchange protocols also remove them from the realm of practicality for a BLE-based IoT environment.

Finally, even if a suitably cheap encryption algorithm were used, devices scanning for BLE advertising messages in dense public spaces may receive many unwanted messages, putting further strain on the already overburdened energy and computational resources of the device if all of those messages need to be decrypted or authenticated. However, determining what messages are useful **prior** to decrypting that data is a challenging problem.

D. Privacy in Public IoT Spaces

While encryption can ensure the actual data cannot be read by others, ensuring a user's privacy goes beyond secure communication via encryption. By merely shadowing a user, collecting information on the patterns of transmissions as well as MAC addresses, users can be identified [8]. To eliminate this problem, BLE devices can be configured to rotate MAC address for every advertising message. Essentially each new message looks like it is coming from a different user.

However, total privacy is also not desirable. With some personal information, a retail store could customize offers for particular users if it can identify those users and their buying habits. Incognito supports such limited information sharing [4], setting the BLE MAC address on a user's device to a temporary location-based ID. Unfortunately, Incognito and similar solutions (*e.g.*, [9]) use these temporary identifiers for long enough that short-term shadowing and tracking can still be a problem. The Lamina system solves this problem through the use of shared secrets exchanged during registration and unique MAC addresses per message.

One thing to note is that such privacy concerns are unidirectional. The tags in a public IoT space do not need to maintain this type of privacy, only users within the public IoT space need such protection. This asymmetry allows tags in the pubic IoT space to use the same MAC address for indefinite periods of time. Thus, the user's mobile devices can easily detect repeat messages, not wasting energy on processing messages already seen as discussed in Section III-A3.

III. The Lamina Architecture

To enable the goal of secure and privacy-preserving communication in public IoT spaces, the Lamina architecture is designed around three primary components: a cloud component for user registration with a public IoT space; a user device module for providing encryption and privacy; and a public IoT space module for providing encryption (see Figure 6). As discussed in detail below, users, upon entering a public IoT space (*e.g.*, a retail store), utilize Lamina cloud registration to exchange shared secrets and other information to support interactions between the user device and the public IoT space. During further interactions with the IoT space, Lamina ensures privacy and security while ensuring the IoT space has sufficient information to deliver targeted recommendations and services (*e.g.*, targeted coupons, directions to a friend's favorite painting).

To control exposure of user information, Lamina divides the world into separate location-based IoT spaces, similar to Incognito [4]. This could be different stores, museums, or airports. A user registers separately for each IoT space in which it would like to receive services. In this context, IoT spaces become a logical collection of IoT-enabled objects. For

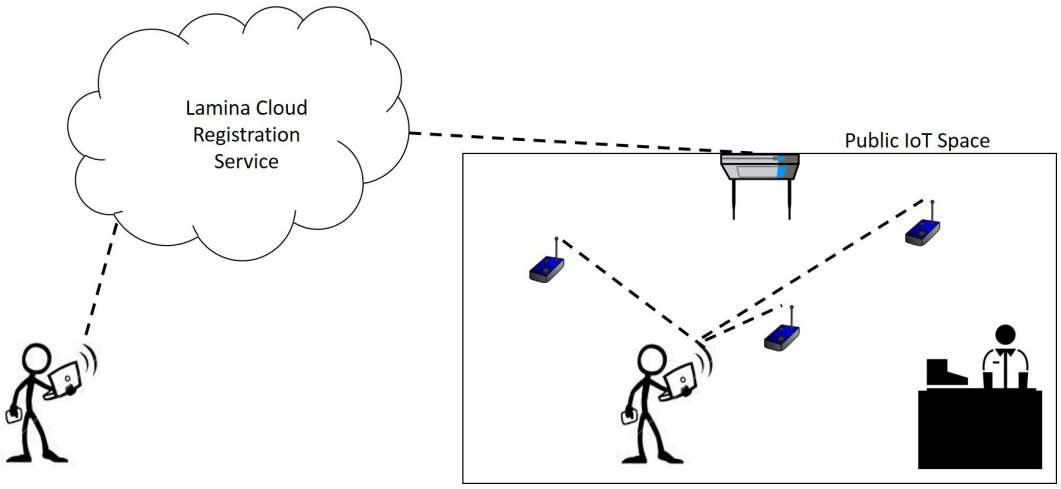

Fig. 6. Lamina Architecture: Cloud Registration Service, User Devices, and Public IoT Space

example, a single retail store may be a public IoT space. Alternatively, an organization may choose to create a single public IoT space that encompasses all of its retail locations. Public IoT spaces are not necessarily only retail spaces. For example, a city may create a public IoT space representing all of its parks or a museum might create a public IoT space.

A. Lamina Device Modules

Lamina must support personal devices carried around by the user as well as infrastructure and environment devices deployed by the manager of the public IoT space. A user's devices must be able to collect data from the public space in a trustworthy manner. Additionally, these devices act as advertisers for the location and personal information of the user. On the IoT environment device side, advertising tags can be deployed throughout the public IoT space to enable interactions with the users in the environment. Such information may include specific deals or coupons for access only by a subgroup of users. To support such targeted communication, the tags must implement security mechanisms that can act as an authentication of the user. As a user moves around the IoT-enabled space, the user's device collects data by listening to advertising messages from the tags. While it is certainly possible for a user device to utilize more than one radio technology to perform this scanning, our initial design of Lamina is implemented using only BLE. However, the techniques built into Lamina can be extended to other wireless protocols, which we intend to explore in future work.

In the face of potentially huge numbers of tags in any public IoT space, coupled with the fact that numerous users are expected to be in each public space, Lamina minimizes the potentially massive energy drains associated with a high density of BLE objects in an environment by utilizing energy-efficient CryptoCoP-based encryption and by nonce-based filtering to determine which messages should be processed from the public IoT space. These two mechanisms ensure energy efficient processing while maintaining the desired security and privacy guarantees.

1) Lamina: CryptoCoP-based Encryption: To provide data security, Lamina implements CryptoCoP-based encryption [10] on both user devices and tags throughout the environment. CryptoCoP utilizes AES [11] in Counter (CTR) mode [6], which uses a counter value to maintain synchronization between the cipher stream at the sender and the receiver. This counter mode allows the stream cipher to operate in the face of losses. Essentially, no message in the stream of messages requires the successful reception of **previous** or **subsequent** messages for successful decryption. However, the counter value must be shared for decryption to be successful, but does not have to be kept secret. Essentially, the integration of CryptoCoP into Lamina guarantees successful decryption for any message actually received.

CryptoCoP relies on a single 256 B shared secret key, a shared nonce, and a counter value for its AES CTR mode encryption. The shared secret keys and shared nonces (collectively "keying material") are exchanged during registration as described in Section III-B below. Essentially, the user device generates a key and nonce that it will use for encryption of its messages and the public IoT space generates a key and nonce that it will use. These sets of keying material are exchanged during registration and used for encryption and decryption throughout the time the user device is interacting with the public IoT space.

Figure 7 depicts the modified iBeacon [12] packet format used by CryptoCoP. CryptoCoP replaces the Major, Minor, and TX Power fields with a single field containing the 6 B counter value. This change removes components that leak information that can be used to defeat privacy and allows more room for the actual encrypted data block. For example, the TX Power field can be used to estimate the distance a particular sender is from a scanning device overhearing the transmission. This is undesirable for obvious privacy reasons.

2) Lamina: CryptoCoP-based Privacy: In public IoT spaces, privacy is only a concern for user devices. Environment tags do not need protection from being identified by third

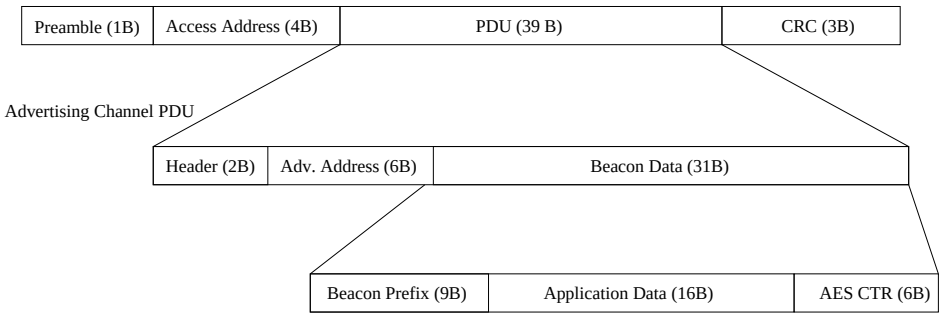

Fig. 7. CryptoCoP Packet Format

parties. On the contrary, they are typically well identified (*e.g.* consider a Smart LaBLE on a retail shelf). Thus, Lamina only implements privacy mechanisms to protect user devices. This simplifies the steps a user's device must take to effectively filter out unneeded messages (see Section III-A3 below).

To preserve privacy for the user devices, the MAC address of each user device is altered for each message transmission. The specific MAC address for each message is generated by hashing the <shared nonce, counter> tuple using the Secure Hashing Algorithm (SHA). The shared nonce is exchanged during device registration with the IoT space as described in Section III-B and the counter value is included in the message header (see Figure 7). Therefore, the IoT space has all of the necessary information to correlate messages from the same user. However, third parties attempting to shadow a user through the IoT space, not having access to the shared nonce, will not be able to correlate the transmissions. Additionally, without access to the TX power field, which CryptoCoP removes, a shadowing device will have difficulty estimating the physical proximity of a transmitting device.

Tags in the IoT space, on the other hand, do not rotate their MAC addresses. Each tag in a particular IoT space is assigned a unique tag identifier. This identifier can then be used to correlate all messages from a particular tag.

3) Lamina: Nonce-based Filtering: To avoid unnecessarily decrypting messages not targeted to a specific user, user devices utilize two pieces of information to filter incoming messages: the shared nonce and a tag identifier that is unique within a particular public IoT space. Tags throughout the public IoT space make use of the same CryptoCoP-based encryption as the user devices, but there is no privacy concern as to the **identity** of the tags as discussed above. Therefore, the tag MAC addresses are not cycled using the CryptoCoP privacy algorithm. However, simply using the unique tag identifier as the MAC address would still carry with it the potential of forcing a user device to decrypt information not targeted to that user. For example, a particular tag may be configured to transmit three different levels of coupons, each aimed at a different group of users. By utilizing a hash of the shared nonce in addition to the tag identifier, the MAC address can be used to filter messages intended for the user from each tag in the IoT space. The shared nonce used by the tags is not the same shared nonce as that used by the user devices. This is important so that each tag can use potentially one shared nonce for an entire group of users (*i.e.* every user in the group would receive the same keying material from the IoT space during registration). Thus, as discussed in Section III-B, two shared nonces are exchanged during registration.

Finally, messages themselves need only be decrypted if they are received from a unique <MAC address, counter> tuple. Essentially, a transmitting tag in the environment will only increment its CryptoCoP counter when it transmits a **new** message. Therefore, upon receiving a message, a user device looks to the MAC address to determine whether the message is intended for it (*i.e.* has it been encrypted by a known key) and looks to the counter value to determine whether it is a new message. Only after passing these two tests, based on simple comparisons, will the user device execute the decryption algorithm.

B. Lamina: Cloud Registration Service

One key problem with utilizing shared secret-based security techniques is that the communicating parties must share a secret in advance. Also, to preserve the ability of the public IoT space to identify users to provide them with targeted information and services while using MAC address rotation to ensure privacy, both the IoT space and the user must agree on a MAC address rotation scheme. This scheme obviously must also be a shared secret between the IoT space and the user so that third parties cannot determine the identity of a user by the MAC address rotation. Both of these issues involve sharing secrets between the user and public IoT space **prior to** interacting with the space.

In a retail scenario, Lamina facilitates the ability of a retail store targeting coupons and other deals to specific customers in real time as the customer moves around the store. The store can encrypt certain coupons as to only be accessible by a specific, targeted groups of customers. Additionally, information regarding preferences and interactions within the store from the customer is encrypted so that only the IoT space can access that information. Finally, as described in the previous sections, shared nonces are used to provide MAC addresses and a MAC address cycling protocol for protecting the identity of the users.

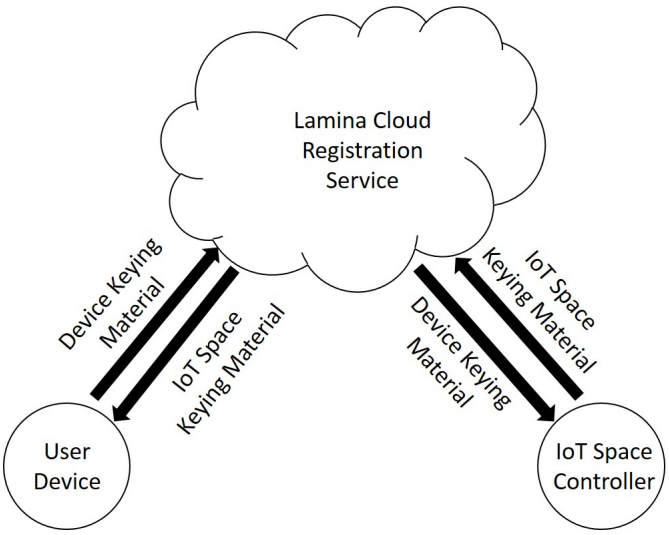

Fig. 8. Cloud Registration Service

To facilitate these features, Lamina uses a cloud-based registration service. Prior to entering a desired public IoT space such as a store, a customer utilizes their device (*e.g.*, smartphone or smartwatch) to access the store's cloud-based registration service. Lamina uses out-of-band registration as a further step to prevent shadowing within the store. Currently, MAC address rotation is not well supported in WiFi base stations. Instead, a device must re-associate with a base station every time it changes MAC addresses. Thus, the use of WiFi within the store would expose the customer to tracking and identification by third parties. We will explore extensions to WiFi to support Lamina privacy features in future work.

Figure 8 depicts the Lamina cloud registration service. The user device connects to the registration service, for example by using an LTE radio, and provides a shared nonce and shared 256 B key to the public IoT space. The public IoT space (via an IoT space controller) provides a shared nonce and shared 256 B key to the user device in return. In addition to the shared secrets, the public IoT space can request any other data for specific tracking applications, such as a rewards card number, phone number, or username. To securely share this information, HTTPS is used for the entire cloud connection. Once this information exchange is complete, the public IoT space is prepared to provide targeted information and services to the user in a secure manner.

IV. Lamina In Action

To support both targets of security and privacy, Lamina must be implemented on both the user devices as well as the tags throughout the IoT space. While Lamina can be deployed directly onto the tags used in a public IoT space, an implementation of Lamina on a smartphone or smartwatch will likely be, at least in part, at the level of an app. If the app is not carefully implemented, information could be unintentionally leaked to the third parties. Additionally, energy consumption on a user's devices must be minimized, including any impact of Lamina on that energy consumption. In this section, we explore both implementation issues and Lamina's impact on energy consumption.

A. Lamina on the User Device

Lamina extends our prior work on Incognito to support the storage of shared secrets. Incognito included a system component that was installed on a user's smartphone or smartwatch and was responsible for managing user device identities. These identities were exposed to various IoT environments to control the amount of information exposed to those environments [4]. In Lamina, a system component is needed not to store identities themselves, but instead to store the shared information (nonces and keys). This shared information is then used by Lamina to create new MAC addresses (identities) for each transmitted message. The Lamina system component is also in charge of managing the shared key and nonce store. A decision must be made as to how often to reuse the keying material. For example, keying material could be different for every individual public IoT space, or for every day, or every hour. Essentially, there is a trade-off between the potential for a third party to be able to learn the keying material and its reuse. Incognito provided a system framework for the user to control the level of information exposed to particular space. This same framework is used by Lamina to allow users to choose keying material reuse parameters.

Keying material generation relies on pseudo-random number generation and an AES algorithm. As will be shown in the next section, although the AES algorithm has minimal impact on the energy consumption of a device, experiments have shown that the key generation itself can be expensive in terms of computation and, therefore, energy consumption. As a result, preloading keying material can save significant energy [10]. The amount of keying material that can be preloaded depends on the storage capacity of the device, which obviously impacts the length of time Lamina can function (or alternatively, the number of public IoT spaces that can be visited) prior to new keying material being required.

Additionally, the Lamina system component must manage the actual encryption of outgoing messages, the MAC address generation, nonce-based message filtering, and message decryption algorithms. All of this functionality must be transparent to IoT applications built on top of the Lamina system for the user devices.

B. Impact on Energy Consumption

The main cost added by Lamina is the use of CryptoCoP-based encryption. We have shown that CryptoCoP adds negligible energy consumption as compared with no encryption.

We compared the average energy costs to generate and send a 16 byte message using no encryption, using a pre-generated keystream with a simple XOR procedure, and with the full CryptoCoP algorithm with on-device key generation for each message. As can be seen, the full CryptoCoP algorithm only increases the energy consumption by 0.07% over no encryption. Such a negligible increase should have no appreciable

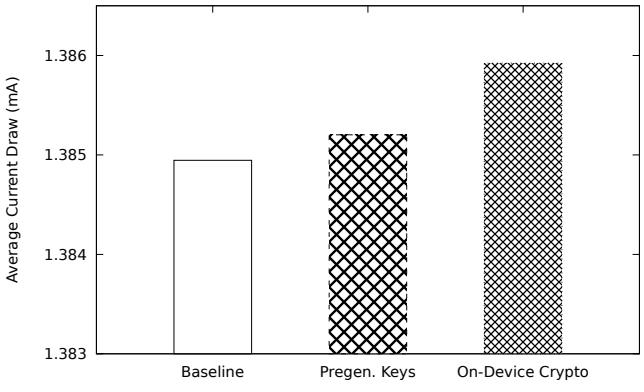

Fig. 9. CryptoCoP Encryption Energy Consumption

impact on battery life for user devices. Thus Lamina does not negatively impact user device uptime.

Another point to note is that the comparison of MAC addresses and nonces to determine whether or not a message should be decoded uses an average of 1/1000 of a milliamp. Again, the operation is virtually free in terms of energy consumption.

C. Lamina Impact on Users

There are essentially two sets of users from the perspective of Lamina. First, there are the users in the IoT spaces. Second, there are the owners of the public IoT spaces themselves. Given current trends, people are willing to expose certain information to a space, such as a retail store, in exchange for tangible benefits, such as targeted coupons (*e.g.*, discount gas cards and other reward cards). However, users prefer to affirmatively choose to share such information (*e.g.*, people want to affirmatively apply for rewards cards) and have the ability to "opt-out." The cloud registration system used in Lamina provides a parallel mechanism to that used by physical rewards cards. Users choose to affirmatively register with a public IoT space. If they choose not to register, they can obviously still physically be in the space (for example by walking through the store); however, they will not get the benefit of targeted information and services provided by the public IoT space.

Users are becoming more aware of the dangers inherent in letting too much of their personal information leak into the hands of third parties. Therefore, Lamina's mechanism to securely control the information provided to the public IoT space while still protecting that data, and indeed their identity, from snooping third parties helps alleviate such concerns, encouraging users to make use of the benefits of the public IoT spaces.

From the perspective of the owners of the public IoT spaces, at first, it may seem that Lamina prevents simple discovery of a large amount of identifying information. For example, it provides the possibility of users simply not allowing a space to track their movements (if a user refuses to register with a space). However, we believe the extra layer of security will encourage more users to take part in information sharing with trusted public IoT spaces, giving the spaces the benefit of collecting richer statistical information about their customers. By potentially providing a standard platform on which IoT spaces can be built, organizations can focus on developing rich IoT experiences without having to prove to customers that each individual solution is adequately secure. This is a potentially large benefit as society becomes more security and privacy conscious.

V. Conclusion and Future Directions

In this paper, we presented Lamina, a mobile system that enables privacy and security for user device interaction in public IoT spaces. Lamina includes an out-of-band, cloud-based registration system where keying material is exchanged between the user device and the desired public IoT space. Once the keying material is exchanged, CryptoCoP-based encryption and MAC address cycling are used on the user device to ensure third parties cannot obtain private information regarding the user that is shared with the IoT space. Lamina also ensures that the public IoT space can acquire enough identifying information regarding users traversing the space to provide targeted information and services while still protecting the users' identities.

Our future directions include integrating the ability to control the level of information shared with the IoT space from the user application. In previous work, we developed such a system, called Incognito. Full integration of the Incognito system with Lamina would accomplish this task. Additionally, the privacy mechanisms utilized by Lamina involve rotating MAC addresses, which are calculated as hashes of shared secret information. Lamina implements this technique in a BLE environment. Extending the technique to other wireless technologies, such as WiFi, would require modifications to the base stations. Currently, upon a MAC address change, a WiFi devices must re-associate with the base station. This is undesirable from both a continuity of communication perspective as well as from an energy consumption perspective. We intend to explore altering the protocols used at the base stations for association to support the Lamina/CryptoCoP privacy mechanisms. Finally, we plan to build a full targeted coupon delivering application and deploy Lamina on a testbed that models a retail environment. Using such a testbed we can fully test issues related to latency and a user device's interactions with multiple IoT tags in a single IoT space.

Acknowledgments

This research is funded in part by a Focused Research Grant from Google, Inc.

References

[1] nrf51822 bluetooth smart beacon kit. http://bit.ly/1L34QCz.

[2] Google Inc., "Physical web." [Online]. Available: https://google.github.io/physical-web/

[3] G. Tuncay, V. Khanna, R. Kravets, and A. F. Harris III, "Smart vending: Iot-enabled inventory control (demo)," in *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications (HotMobile)*. ACM, 2016.

[4] R. Kravets, G. Tuncay, and H. Sundaram, "For your eyes only," in *MCS*, 2015.
[5] IETF, "RFC 5246: The Transport Layer Security Protocol Version 1.2."
[6] NIST, "NIST Special Publication 800-38A. Recommendation for Block Cipher Modes of Operation," 2001, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf.
[7] G. de Meulenaer, F. Gosset, F. X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks," in *2008 IEEE International Conference on Wireless and Mobile Computing, Networking and Communications*, Oct 2008, pp. 580–585.
[8] A. Das, P. Pathak, C.-N. Chuah, and P. Mohapatra, "Uncovering privacy leakage in ble network traffic of wearable fitness trackers," in *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications (HotMobile)*. ACM, 2016.
[9] M. Arapinis, L. Mancini, E. Ritter, and M. Ryan, "Privacy through pseudonymity in mobile telephony systems," in *NDSS*, 2014.
[10] R. Snader, R. Kravets, and A. F. Harris III, "Cryptocop: Lightweight, energy-efficient encryption and privacy for wearable devices," in *WearSys*. ACM, 2016.
[11] NIST, "Federal information processing standards publication 197. Advanced Encryption Standard (AES)," 2001, http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[12] Apple. (2014) Getting started with ibeacon. http://apple.co/1MPb7CU.