ALLEGION
PIONEERING SAFETY™

SCHLAGE

ENGAGE Wireless (BLE & Wi-Fi) Security White Paper

June 2020
Version 2

Joe Baumgarte
Principal - IoT Security Engineer
Allegion plc
Hague Road Technical Center
8750 Hague Road
Indianapolis, IN 46256
Joe.baumgarte@allegion.com

KRYPTONITE ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

Table of Contents

1. ABSTRACT 3
2. INTRODUCTION BLUETOOTH® 4
   - 2.1 BLUETOOTH® CLASSIC 4
   - 2.2 BLUETOOTH® CLASSIC VULNERABILITIES 4
   - 2.3 BLUETOOTH® LOW ENERGY 5
   - 2.4 BLE VULNERABILITIES 5
3. FOUNDATION OF ENGAGE™ BLE SECURITY 6
   - 3.1 SECURITY AND PRIVACY BY DESIGN 6
   - 3.2 BUILT ON PROVEN SECURITY PRACTICES 6
   - 3.3 SECURITY UPDATES AND VULNERABILITY MANAGEMENT 7
   - 3.4 TESTED BY INTERNAL AND EXTERNAL EXPERTS 7
4. SECURITY OVERVIEW 7
5. ENGAGE™ BLE COMMUNICATION CONSISTS OF MULTIPLE SECURITY LAYERS 8
   - 5.1 LAYERED SECURITY 8
   - 5.2 INNER LAYER – PRODUCTION KEY 8
   - 5.3 LOCAL LAYER – SITE KEY 8
   - 5.4 BLE COMMUNICATION LAYER – TEMPORARY KEY 8
   - 5.5 GATEWAY COMMUNICATION – GATEWAY KEY 8
   - 5.6 ENGAGE™ BLE AUTHENTICATION 9
6. CONCLUSION 9

1. Abstract

ENGAGE™ Wireless Technology uses combinations of AES-256 bit keys and encryption methodologies to prevent wireless (Bluetooth® Low Energy or Wi-Fi®) attacks against ENGAGE™ enabled devices. These methods prohibit unauthorized access to any device, its configuration, or its programming. While it is possible to connect to any ENGAGE™ device via Bluetooth®, it is not possible to maintain the connection or make changes to the device without utilizing the patented ENGAGE™ Security Protocol.

2. Introduction Bluetooth®

2.1 Bluetooth® Classic

Bluetooth® is a wireless protocol that has formally been around since the mid to late 1990's and has taken on many connotations as people have adapted to its very prolific usage in various forms. The reason for the proliferation of the technology and protocol is its ability to coexist with other signals in the 2.4 GHz ISM (Industrial, Scientific, and Medical) license-free band. It does this, partially through the Adaptive Fast Frequency Hopping technology that enables it to dynamically use only those of the 80 channels that can allow it to get a good signal through the busy 2.4GHz band and because of how inexpensive the technology-itself is. The combination of the two has enabled Bluetooth® to become arguably the most prolific wireless technology alongside Wi-Fi®.

The form of Bluetooth® enabled devices that most people use are the many devices that attach (technically called a bond or a pair) to cellphones to enable wireless audio. This can take the form of headphones to wirelessly pass music audio data, often for the purposes of having music while running or exercising (technically called the Advanced Audio Distribution Profile) or using a headset for making wireless phone calls to an earbud or similar device (technically either the Headset Profile or the Hands-Free Profile). These profiles were introduced in Bluetooth® 2.0 and are associated with Bluetooth® Classic which is not related to Bluetooth® Low Energy in any meaningful way. Finally, the encryption of Bluetooth® Classic is a customized encryption based upon a block cipher called SAFER+. Bluetooth® uses a custom encryption cipher and once the encryption has been established, is generally considered safe.

2.2 Bluetooth® Classic Vulnerabilities

The most common vulnerabilities associated with Bluetooth® Classic are seen during the pairing process. The principle vulnerability is how devices are "detectable"; for Bluetooth® Classic devices, it is important that devices NOT be permanently detectable. It is for this reason that you have to put your devices into a "pairing mode" to enable them to be detected – this prevents others from pairing with your devices and further prevents you from being "tracked" through a building by following those messages. Further, this prevents others from sending malicious information to your cellphone.

The second most-common vulnerability is related to the difficulty of pairing with Bluetooth® Devices. For most Bluetooth® devices that people commonly use, there are only buttons, there isn't a display to convey any information, so it is very common for devices to have "0000" or "1234" as their pairing password. Obviously, these are easy numbers to guess, which is why it is critical to keep the pairing time (first-vulnerability) limited. Wirelessly, the combination of the two vulnerabilities, at the time of pairing, can give an attacker unlimited access to the data being transmitted in both directions.

These are the two most common attack points for Bluetooth® Classic. It is for this reason that cell phone and Bluetooth® device manufacturers have made it so that generally Bluetooth® is

non-discoverable by default and you must enable discoverability in order to pair. Unfortunately, due to the name "Bluetooth®" it is easy to assume that these recommendations apply to BLE, even though it is a very different protocol.

2.3 Bluetooth® Low Energy

Bluetooth® Low Energy (BLE) was introduced in the Bluetooth® 4.0 specification, but it is different than Bluetooth® Classic in virtually every way. From the number of wireless channels in the protocol (40), to the method of coexistence in the wireless spectrum, even the method of encryption used (AES-128) is different between the two protocols. BLE is common to Bluetooth® Classic only by the fact that it is named Bluetooth®. It fundamentally is a different wireless protocol, which happens to use the same 2.4 GHz band for communication.

BLE uses a defined structure of devices in order to achieve its low power efficiency. Generally, the device that needs to be the lowest power device is called a "peripheral." By the standard, a peripheral is always advertising its services allowing the other devices in the system (typically a "central" or a "scanner") to detect the peripheral and establish a connection if desired. Common examples of peripheral BLE devices are wireless keyboards, Air Pods®, or personal fitness devices such as a Fitbit® or the H7 Polar Heart Rate Monitor. In fact, no matter where you are, if you turn on your Bluetooth® and perform a search, you'll likely find someone with a Fitbit®, or other BLE device, within range; this is normal and unavoidable. However, unlike Bluetooth® Classic, this isn't something to be avoided because the system was designed to operate in this way.

The system is designed to allow the peripheral to use very little energy until it is connected, allowing for a highly responsive system where a user doesn't need to first power the device on before it can be used, but still give terrific battery life when not in use. When a central connects to a peripheral, the peripheral enters a higher-powered state; in this state, the advertisements do stop, but the device is now drawing more power because the system is now fully operational.

2.4 BLE Vulnerabilities

The primary vulnerability is the ease of which a BLE peripheral is designed to connect to a BLE central. One effect of the peripheral/central architecture is that the peripheral has no information about the central until a connection is made; unfortunately, this is true of every BLE connection. For this reason, many BLE devices do not require "pairing" and will respond to any device connected to it.

The second vulnerability was discovered shortly after the standard was released. Although the system uses AES-128 encryption, it is possible to force the connection to re-negotiate the key exchange during communication. By monitoring the key exchange, it is possible to determine the key being used and monitor 100% of the data being exchanged during communication.

3. Foundation of ENGAGE™ BLE Security

At Allegion™ (parent company of Schlage), we strive to provide seamless access and a safer world. Security and privacy are at the core of what we do and what we think about every day. We take a broad and deep approach to ensuring safety and security to protect the devices, products and systems that, in turn, protect people and assets wherever they reside, work and thrive. Allegion has a Product Cybersecurity Program that's designed around four key pillars:

3.1 Security and privacy by design

The concept of building security and privacy into technology solutions both by default and by design is a core expectation for Allegion's product development initiatives. Some of Allegion's core security principles in security and privacy by design are:

- Utilize a "Defense in Depth" approach to security through multi-layered security controls;
- Data is protected at rest and in motion;
- It is assumed external systems are insecure;
- Users and processes are authenticated and then their authorization is verified;
- Security is periodically reassessed; and
- Users' right to privacy is respected, and we strive to protect it.

3.2 Built on proven security practices

Security technology is important to security, but the practices of the people who develop that technology are more important. These practices are the foundation of security. It is crucially important that security practices be good ones. A few of Allegion's security best practices include:

- Full-time global cybersecurity team committed to driving security into software and firmware development process;
- Cybersecurity training for all developers and testers;
- Security and privacy requirements defined during requirements phase;
- Threat modeling conducted during design phase; and
- Static analysis tools utilized during implementation phase.

- Source code analysis
- Open source analysis

3.3 Security updates and vulnerability management

Allegion takes security concerns seriously and works to quickly evaluate and address them. Once a security concern is reported, Allegion commits the appropriate resources to analyze, validate, and provide corrective actions to address the issue.

- Firmware updates are encrypted and signed using a cryptographically secure method;
- Security issues are tracked to closure and root-cause analysis is performed;
- Lessons learned are incorporated into the development process to help prevent repeat issues.

3.4 Tested by internal and external experts

To help product teams address emerging security challenges, Allegion utilizes both internal and external experts to conduct penetration testing guided by the OWASP Application Security Verification Standard (ASVS), which provides the range in coverage and level of rigor applied to each product/solution. This testing includes:

- Penetration testing (run-time analysis);
- Reverse engineering (binary analysis);
- Code reviews (static analysis);
- Threat modeling (design analysis); and
- Device testing (hardware analysis).

4. Security overview

All ENGAGE™ devices use BLE as the method of communication with a mobile device. The design team took many factors into consideration in choosing to adopt BLE as the communication protocol to these devices. From the outset, it was determined that no ENGAGE™ device would rely on the BLE security protocol for any communication because the likelihood of that protocol being attacked and hacked was very high. To ensure the security of the ENGAGE™ system, a custom security protocol, using off-the-shelf encryption standards and best-practices, was developed to meet our high security standards. To prove out the security of the method that is used, our devices and protocols have been third-party tested and the protocol has been verified to utilize some of the most secure methods available.

5. ENGAGE™ BLE communication consists of multiple security layers

5.1 Layered Security

Any security analyst will tell you that the best security methodology has layers. Designs that have layered security, rely on the many layers to protect the information that is most-secret. ENGAGE™ was built with this same methodology in mind. Further, every key used in ENGAGE™ is an AES-256 bit key, which has nearly as many permutations as there are atoms in the observable universe – therefore, it is not possible to determine the key by brute force attacks with conventional technology. Finally, no ENGAGE™ device will react to any command or request until all of these layered security needs are met.

5.2 Inner Layer – Production Key

The highest security layer in ENGAGE™ is a unique AES-256 bit key programmed into every device. This key is programmed in an Allegion factory and is known only to Allegion. The purpose of this key is to allow the device to be uniquely captured on the final customer's door and to allow subsequent keys to be securely transmitted to that specific device. The fundamental purpose of this key is to prohibit an attacker from attempting to factory reset and reprogram the lock.

5.3 Local Layer – Site Key

The next layer allows anyone with appropriate access to the ENGAGE™ account to manage access for any device on that account. This unique AES-256 bit key protects all communications and data associated with that site.

5.4 BLE Communication Layer – Temporary Key

This AES-256 key is used to encrypt the data between the mobile application and the device. This key is unique to each mobile device, and to further protect the customer, it expires daily. Therefore, each mobile device is daily issued a unique key to allow it to communicate with ENGAGE™ devices. This key is no longer accepted after that day and the mobile device will need a new one. This is among the reasons why the ENGAGE™ mobile application requires access to the internet in order to operate.

Further mechanisms are in-place to prevent replay attacks against any device preventing attempts to reuse this key at any time, or to even prevent reuse of an entire communication sequence.

5.5 Gateway Communication – Gateway Key

When connected to an ENGAGE™ Gateway, yet another unique AES-256 bit key is used for all communication between that Gateway and the connected edge devices. The encryption mechanism used is dynamic, meaning the key is changed with every single message! This

further prevents any replay or eavesdropping attacks because a different encryption key is used with every message.

5.6 ENGAGE™ BLE Authentication

ENGAGE™ devices use a patented, layered security algorithm with multiple security keys in order to authenticate devices before communicating with them using BLE. Only after authentication does the device allow any information to be sent or gathered. However, recall that the peripheral (ENGAGE™ device) has no information about the central until the communication has been established; this means that any central can connect to an ENGAGE™ device. However, only devices (ex. the ENGAGE™ Gateway) and applications (ex. the ENGAGE™ mobile app) that have the appropriate authentication token, and follow the security protocol, can maintain the connection to perform any operation. It is for this reason that if authentication has not been established within a few seconds of connection to an ENGAGE™ device, the ENGAGE™ device will break the connection.

6. Conclusion

In conclusion, the fact that ENGAGE™ devices communicate at all creates opportunities for attacks to be made, but the ENGAGE™ security protocol was specifically developed to protect against these types of attack. Allegion uses a validated, patented approach to organizing, authenticating, and authorizing all communications to/ from all ENGAGE™ devices. This approach was specifically designed to protect against wireless attacks (ex. sniffing, replay) and is continuously being monitored and updated. Our protocol has had multiple third-parties validate the algorithm being used to ensure the resistance to known attacks.

About Allegion™

Allegion (NYSE: ALLE) is a global pioneer in seamless access, with leading brands like CISA®, Interflex®, LCN®, Schlage®, SimonsVoss® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion secures people and assets with a range of solutions for homes, businesses, schools and institutions. Allegion had $2.9 billion in revenue in 2019 and sells products in almost 130 countries. For more, visit www.allegion.com.. .