ALLEGION
PIONEERING SAFETY™

ISONAS™

Pure Access Cloud Security White Paper

January 2023
Version: 1

Allegion Product Cybersecurity Team
Allegion plc
Hague Road Technical Center
8750 Hague Road
Indianapolis, IN 46256
cybersecurity@allegion.com

KRYPTONITE ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

Table of Contents

1 Abstract

ISONAS™ Pure Access supports a combination of Wired and Wireless technologies. Both technologies use combinations of AES-256 bit keys and encryption methodologies to prevent attacks against devices. These methods are intended to prohibit unauthorized access to any device, its configuration, or its programming. While it is possible to connect to many of the devices, it is not possible to maintain the connection or make changes to the device without utilizing patented Security Protocols unique to Allegion.

1.1 Devices and Technologies

The following devices support connectivity with Pure Access:

- ISONAS IP-Bridge
  - Wired Ethernet with Pure Access IP
- ISONAS RC-03
  - Wired Ethernet with Pure Access IP
- ISONAS RC-04
  - Wired Ethernet with Pure Access IP
- Schlage RC11/RC15/RCK15
  - Wired Ethernet with ENGAGE™ IP
  - ENGAGE Mobile Application with ENGAGE Bluetooth® Low Energy
- Schlage NDEB
  - Wireless Ethernet with ENGAGE IP
  - ENGAGE Mobile Application with ENGAGE Bluetooth® Low Energy
- Schlage LEB
  - Wireless Ethernet with ENGAGE IP
  - ENGAGE Mobile Application with ENGAGE Bluetooth® Low Energy
- Schlage ControlB / ControlBM
  - ENGAGE Mobile Application with ENGAGE Bluetooth® Low Energy

2 Foundation of Allegion Security

At Allegion™ (parent company of both Schlage and ISONAS brands), 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:

2.1 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.
- Users' right to privacy is respected, and we strive to protect it.

2.2 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.
- Static analysis tools utilized during implementation phase.
  - Source code analysis
  - Open-source analysis

2.3 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.

2.4 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, 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)
- Device testing (hardware analysis)

3 Introduction to Bluetooth®

3.1 Bluetooth® Classic

Bluetooth® is a wireless protocol that was formally introduced in 1998 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.

3.2 Bluetooth® Classic Vulnerabilities

The most common vulnerabilities associated with Bluetooth® Classic are seen during the pairing process. The principal 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 one must put devices into a “pairing mode” to enable them to be detected – this prevents others from pairing with one’s devices and further prevents being “tracked” through a building by following those messages. Further, this prevents others from sending malicious information to one’s 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 to pair. Unfortunately, due to the name Bluetooth® it is easy to assume that these recommendations apply to Bluetooth® Low Energy (BLE), even though it is a very different protocol.

3.3 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. Bluetooth® Low Energy 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.

Bluetooth® Low Energy uses a defined structure of devices 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 Bluetooth® Low Energy 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 Bluetooth® Low Energy 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.

3.4 Bluetooth® Low Energy Vulnerabilities

The primary vulnerability is the ease of which a Bluetooth® Low Energy peripheral is designed to connect to a Bluetooth® Low Energy 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 Bluetooth® Low Energy connection. For this reason, many Bluetooth® Low Energy 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.

4 Introduction to IP Communication

4.1 IP Communication over Wired Ethernet Connections

Wired Ethernet was formally standardized in 1983 with the IEEE 802.3 standard, but development stretches back over the preceding decade. Ethernet has evolved to support an array of bit rates (most commonly 10, 100, and 1000 Megabit), a star topology, a variety of cabling types, and a rich tapestry of protocols layered on top. Most commonly, IP Communication protocol is used, which breaks messages into packets which fit into Ethernet frames.

4.2 IP Communication over Wireless Ethernet Connections

Wireless Ethernet was formally standardized with the IEEE 802.11 standard for Wi-Fi in 1997. Subsequent revisions to the standard increased bandwidth and added modulation techniques. These different versions of the protocol support different numbers of channels, channel widths, channel frequencies, and corresponding bitrates. Much like wired Ethernet, a rich tapestry of protocols can be layered on top of Wireless Ethernet, including security layers such as a WPA2 for network authentication, and IP Communication protocol, which breaks messages into packets to fit into Wi-Fi frames.

4.3 IP Communication

Development started in 1974 and continuing today, the widely used IP Communication protocol is used by Allegion devices with both wired and wireless Ethernet. IP Communication has a long, rich history of many different flavors. Common elements include:

Communication is based around packets of data moving through the network

- Packets are delivered from source to host.
- Packets may be relayed across network boundaries using routing.
- Packets may flow across many technologies, including wired Ethernet, wireless Ethernet, DSL, fiber, cable, and many others.
- In the TCP/IP model there are four layers: network access at the bottom most layer, followed by internet, transport, and application layers.
- Billions of devices around the globe interconnect using IP Communication.

4.4 IP Vulnerabilities

Given the diverse eco-system, billions of endpoints, and long-range nature of IP Communication, it is a common target of attack by malicious actors. In virtually all cases, attackers are attempting to compromise one of the three following aspects of communication:

- Confidentiality
- Integrity
- Authentication

Attacks commonly attempt to exploit weaknesses including insecure protocols, poor key or password selection, routing manipulation for man in the middle attacks, improperly crafted certificate chains, buffer overflows, command injection, denial of service attempts, improperly configured firewalls, and others. Many industry groups exist to advocate for IP cybersecurity, including the non-profit Open Web Application Security Project aimed at education and government groups such as the US based Cybersecurity and Infrastructure Security Agency aimed at cataloging known vulnerabilities.

5 ENGAGE™ Bluetooth® Low Energy communication

All ENGAGE devices use Bluetooth® Low Energy as the method of communication with a mobile device, including the ENGAGE devices that operate with Pure Access (Schlage NDEB, LEB, ControlB, and RC11/RC15/RCK15). The design team took many factors into consideration in choosing to adopt Bluetooth® Low Energy as the communication protocol to these devices. From the outset, it was determined that no ENGAGE device would rely on the Bluetooth® Low Energy 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.

5.1 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 Bluetooth® Low Energy 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 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 ENGAGE™ Bluetooth® Low Energy Authentication

ENGAGE devices use a patented, layered security algorithm with multiple security keys to authenticate devices before communicating with them using Bluetooth® Low Energy. 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 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 ENGAGE IP Security

ENGAGE IP communication (both wired and wireless) rely on a defense in depth strategy that consists of multiple layers.

The configuration of the wireless access point that a lock system is connecting to will impact the security of the Wi-Fi connections. In a White Paper titled ENGAGE WiFi Network Requirements Allegion has recommendations on best practices for both security and compatibility with Allegion devices. When configured with recommendations, Wi-Fi access points will use WPA2 to provide both authentication and encryption to Wi-Fi connections.

6.1 Outer Layer – TLS Encrypted IP Communication Layer

ENGAGE uses Transport Layer Security (TLS) version 1.2 to protect all IP connections. The TLS protocol aims to provide confidentiality, integrity, and authenticity of communications using cryptography. It is part of both the transport and the application layer of the TCP/IP model. With TLS, asymmetric encryption based on digital certificate chains is used to establish temporary symmetric keys used for communication. All data flowing across IP connections is then encrypted with these symmetric keys.

6.2 Inner Layer – Production Key

Before use, devices must first be captured using the Bluetooth® Low Energy based ENGAGE Mobile Application, ensuring that the production key is used to transfer the site key and initial configuration into the device. The fundamental purpose of this key is to prohibit an attacker from attempting to factory reset and reprogram the lock.

6.3 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 credentials used throughout the system, allows for authentication of remote endpoints, and allows for encryption of data at rest.

7 Pure Access IP Security

7.1 AES-256 Protected IP Communication

Pure Access IP connections to the Pure Access cloud support encryption using AES-256 with a customer provided pre-shared AES-256 encryption key. The ISONAS Configuration tool can be used to configure ISONAS branded devices with this key ahead of initial connection to Pure Access. For instructions on how to enable encryption, please reference the video Pure Access Encryption. AES-256 cryptography provides confidentiality between devices and the cloud using an encryption that is estimated to take billions of years for current computers to decipher using brute force methods.

8 Conclusion

The fact that ENGAGE and Pure Access devices communicate at all creates opportunities for attacks to be made, but the security protocols employed were specifically developed to protect against these types of attack. This approach was specifically designed to protect against wireless attacks (ex. sniffing, replay) and is continuously being monitored and updated. Our protocols have had multiple third parties validate the algorithms being used to ensure resistance to known attacks.

ALLEGION
PIONEERING SAFETY™

About Allegion

Allegion (NYSE: ALLE) is a global pioneer in safety and security, with leading brands like CISA®, Interflex®, LCN®, Schlage®, SimonsVoss® and Von Duprin®. Focusing on security around the door and adjacent areas, Allegion produces a range of solutions for homes, businesses, schools and other institutions. Allegion is a $2 billion company, with products sold in almost 130 countries. For more, visit **www.allegion.com.**

KRYPTONITE ■ LCN ■ SCHLAGE ■ STEELCRAFT ■ VON DUPRIN

ALLEGION