A Security Analysis of the Lenel BlueDiamond

Quintin Walters[1], Joshua Niemann[1], Connor Leavesley[1], Daniel Capps[1], and Jacob Ruud[1]

[1]Computing Security, Rochester Institute of Technology

May 6, 2020

Abstract

Contactless authentication devices have existed in some capacity since the late 20th century. These devices allow users to authenticate themselves using something they have (smart card, proximity card, mobile device, etc) rather than something they know (passcode, combination, security question, etc) making the end-user less responsible for their authentication. This puts noticeably more pressure on the manufacturers to provide a product capable of providing confidentiality, integrity, and availability for its users. As such, the technology continues to advance as companies come up with newer, more advanced, ways to authenticate securely. In recent years, Lenel corporations has released multiple products under the BlueDiamond name that claim to "enhance freedom of movement in the workplace." /citelenelbluediamondwebsite To date, these devices remain untested by the further research community for vulnerabilities that may lead to a breach of access control. As such, this paper aims to design an experimental process that future researchers may follow to accurately assess the security characteristics of Lenel's BlueDiamond contactless readers. This experiment will follow standard scientific procedure, using multiple tests to verify results and standard units of measurement to score success. Our analysis of these devices concludes that further testing on the subjects of Wiegand, RFID, Bluetooth, and the physical hardware may uncover significant findings.

Keywords

Lenel, BlueDiamond, Bluetooth, BLE, Bluetooth Low Energy, RFID, Wiegand, Reader

1 Introduction

Third-party academic research is crucial to ensuring access control devices receive appropriate field testing. Untested devices can spell trouble for multiple parties if zero-day vulnerabilities are exploited by unwanted individuals. In this case, a breach of access control could lead to unauthorized access to secure facilities and/or compromise of sensitive information. Causing potentially fatal damage to organizations without proper backups in place.

Lenel's BlueDiamond technology has been deployed in commercial, academic, and residential settings. Making it an ideal target for potential threat actors. Our research analyzes these readers from an attackers perspective in an attempt to identify flaws that may lead to unauthorized access. We believe this form of research will help improve the overall security posture of these devices as well as provide Lenel with helpful feedback on how their devices can be assessed by the public.

The rest of the paper creates a foundation on which further research may be conducted. First we will discuss the background and significance of conducting this research in the first place. Second we will discuss related work in this sector that inspired our work on this project. Third we will discuss our research design and methodology behind the experiments we chose to recommend. Fourth we will discuss recommended data measurement and analysis techniques that we believe will yield the most impactful results. Fifth we will discuss preliminary procedure design, novel techniques, and expected timeline to be used in this experiment. Sixth, we will make some preliminary, theoretical, and practical implications to help guide the direction of the experiment. Finally, we will end with our expected outcomes as well as conclusions to be drawn from this experiment.

2 Background & Significance

Throughout history, people have tried to gain access restricted areas. [1] Locks were created in order to restrict access, but locksmiths were often skeptical of their inventions, and if they could be bypassed. The first documented case of lock picking was a challenge released by Joseph Bramah, an Enlish locksmith. Bramah had just developed his so called safety lock. His lock had safety features that he believed to be completely secure. Obviously, nothing is ever completely

secure, but Bramah put it to the test by announcing a contest. Anyone who could break into his new creation would net a cool sum of 20,000 pounds.

While the Bramah challenge was still in place, another locksmith caught wind of Bramah's idea. Jeremiah Chubb built a lock that would alert an owner if any sort of picking had been detected. He too, announced a challnge. An American Locksmith named A.C. Hobbs took up the challenge, and had it open within an hour of touching the lock. However, that wasn't the only challenge he accepted. Chubb took a trip over to Hobbs' locksmithing shop, and 70 years later, picked the Bramah security lock.

New technology leads to new innovation. Almost overnight, businesses and organizations started using electronic locking systems for their ease of use and simplicity in granting or denying access. Granting access to a building is as simple as a few button clicks. For most organizations, it is much easier to spend the extra money for a digital system with computer-controlled access control than to re-key a lock every single time an employee leaves the organization.

Lock Picking may be a thing of the past, but the security of electronic locks still need to be audited. With most RFID-based systems, like those in locks, cloning cards is easier than ever due to new tools like the ProxMark RFID toolkit.[2] Even though the physical element of locks and lock picking may not stay the same with these newer electronic locking systems, the spirit stays alive in the hacking community. These locks aren't invulnerable, and security professionals can certainly help bring them to the point where they can withstand basic attacks.

3 Related Work

There has been much research done into attacking BLE devices. Several attacks stood out for their exploitation of vulnerabilities and under developed security features while developing an understanding of the Bluetooth security landscape.

Firstly, Generic Attribute Profile (GATT) attacks are a significant first step in attacking any Bluetooth device. By copying the GATT, an attacker can mimic a Bluetooth device and fool applications into connecting to them. In Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks, Robberts and Toft use gattacker to examine Bluetooth advertisements and discover the services and characteristics of the lock. This information is then used to create a copy of the lock and conduct Man-in-the-Middle attacks and test authentication edge cases [3].

O'Sullivan builds on the vulnerabilities present in BLE communication protocol. He explains that the BD ADDR field could be fuzzed to determine the source of the communication and forge a connection to it [4]. Ryan notes that the underlying encryption protocol of BLE is fundamentally weak and allows for attackers to brute force the Temporary Key. An attacker can use that Temporary Key to derive the Long Term Key and break the encryption of the protocol [5].

It can be seen in the literature on BLE is very vulnerable to man-in-the-middle attacks, denial of service, packet sniffing, and other vulnerabilities. Even though higher levels of security are included in newer BLE versions, such as ECC or out-of-band key exchanges, security settings like PINs are still used by manufacturers [6][7][5]. A basic attack chain has emerged in the literature where the GATT is copied and an attack is launched to clear the device's Bluetooth pairings [7]. The device is then tricked into pairing with the malicious device. The handshake is sniffed by the attacker allowing for encryption to be broken.

Other protocols for IoT communications are not free of issues either. Chung shows the Wiegand is still vulnerable to a decade old attack in modern devices. An attacker can intercept and then duplicate the signals sent by a Wiegand device to the control server. This attack can capture and repeat and authorized card without needing to physically duplicate the card [8]. Hakamaki and Palomaki discuss a number of existing RFID attacks that still exist in modern RFID readers [9].

4 Research Design & Methodology

Our research seeks to analyze the security posture of the readers as they would appear in a customer environment. As such, our research design follows a quasi-experimental structure, meaning only pre-existing configurations of the reader will be studied. Setup of the reader for testing will require connecting the power and ground wires to a 12v power source and the D0, D1, and tamper wires to a raspberry pi. Interfacing with a raspberry pi allows researchers flexible access to perform multiple different tasks such as collecting data or changing configurations. Our proposed connection will allow for easy analysis of the Wiegand hardware within the device. Researchers may also choose to set up the BlueDiamond mobile app to allow the

ability for testing bluetooth traffic sent and received by the device. The attack vector serves as a variable in this equation as its outcome can be scored against others using a common standard. Observations of consistency, difficulty, and threat level will allow us to score each attack vector using the Common Vulnerability Scoring System (CVSS) [10].

4.1 Data Measurement & Analysis

As this is primarily a penetration test of the Lenel BlueDiamond, there are four quantitative metrics of note: number of vulnerabilities, severity, likelihood, and risk. A vulnerability is counted if it could be exploited for an unintened effect. The severity, likelihood, and risk can be properly measured by the Common Vulnerability Scoring System, or CVSS 3.x. This would allow for a more uniform scoring standard inline with what the industry uses. Vulnerabilties will be discovered by a number of tools, including devices like the Ubertooth, manual tool usage, and fuzzing. Vulnerabilities found would be sorted based on protocol and CVSS score. This would allow for a clearer picture into the vulnerabilities for each protocol and the risk associated with using them. Once a vulnerability is discovered, an exploit would be attempted to practicality. Practicality is to measure the ease of attack. It is directly proportional to the likelihood, and provides further insight into likelihood than a CVSS score can.

4.2 Procedures

Words

4.3 Timeline

Words

4.4 Novel Techniques

Words

5 Preliminary Suppositions & Implications

Words

5.1 Theoretical Implications

Words

5.2 Practical Implications

Words

6 Expected Outcomes

Not every penetration test finds a massive zero day vulnerability. However, that doesn't mean a test isn't completely useless. Tests may not often discover massive issues, but smaller issues are often prevalent. Issues such as weaker cryptography, issues with bad hardware intrusion detection, and bad endpoint security on older protocols are commonplace. It should be expected to find several smaller issues rather than major flaws in the firmware or the device itself.

Overall, we expect such a test to provide a concrete and detailed analysis on the Physical, Weigand, RFID, Bluetooth, and Networking stacks embedded in the device. Such a test would outline how these protocols work on a device, and provide concrete analysis of potential vulnerabilities and weaknesses found in the implementation.

7 Conclusions

Throughout this paper, we have discussed how to design a testing framework for attacking modern electronic locking technologies. We listed out different types of attacks that could be run against a bluetooth-enabled locking solution. Bluetooth attacks were discussed, along with RFID attacks, and the cryptographic attacks underneath both attack vectors.

We also discussed attacking the device from the backend, from the protocols that allow for the lock to communicate securely with an authentication server. This includes the Wiegand protocol, which is not designed with a security focus in mind.

Lock picking may not yet be on the decline, but electronic locking mechanisms allow for greater viability for most organizations. Overall, electronic locking solutions will be used far into the future. It's heavily important to test these locks to verify that the cryptographic and security mechanisms of these locks are structurally sound.

8 Acknowledgements

We would like to thank Lenel for access to their BlueDiamond reader and their permission to conduct a test of the reader's security posture.

9 References

[1] R. Mars. (2015) A history of lock-picking, from 99 percent invisible and roman mars. [Online]. Available: http:

//www.slate.com/blogs/the_eye/2015/04/15/a_history_of_lockpicking_from_99_percent_invisible_and_roman_mars.html

[2] P. Fraga-Lamas and T. M. Fernández-Caramés, "Reverse engineering the communications protocol of an rfid public transportation card," in *2017 IEEE International Conference on RFID (RFID)*, 2017, pp. 30–35.

[3] C. Robberts and J. Toft. (2019) Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks. KTH. [Online]. Available: https://pdfs.semanticscholar.org/3eb1/c453464f50c30b2dfb2aff705d45bfe7a6d1.pdf

[4] H. O'sullivan. Security vulnerabilities of bluetooth low energy technology (ble). tufts university. [Online]. Available: http://www.cs.tufts.edu/comp/116/archive/fall2015/hosullivan.pdf

[5] M. Ryan. (2013) Bluetooth: With low energy comes low security. [Online]. Available: https://www.usenix.org/system/files/conference/woot13/woot13-ryan.pdf

[6] A. M. Robles-Cordero, W. J. Zayas, and Y. K. Peker, "Extracting the Security Features Implemented in a Bluetooth LE Connection," in *2018 IEEE International Conference on Big Data (Big Data)*, 2018, pp. 2559–2563.

[7] A. C. T. Santos, J. L. S. Filho, A. I. S. Silva, V. Nigam, and I. E. Fonseca. (2019) Ble injection-free attack: A novel attack on bluetooth low energy devices. [Online]. Available: https://nigam.info/docs/jaihc19.pdf

[8] B. Chung. (2017) Wiegand Protocol Access: A Decade of Decryption. Tufts University. [Online]. Available: http://www.cs.tufts.edu/comp/116/archive/fall2017/bchung.pdf

[9] T. Hakamaki and H. Palomaki. (2015) Security of rfid-base technology. [Online]. Available: http://amies-2015.international-symposium.org/proceedings_2015/Hakamaeki_Palomaeki_AmiEs_2015_Paper.pdf

[10] [Online]. Available: https://nvd.nist.gov/vuln-metrics/cvss