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 5, 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." [1] 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

Words

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 [18].

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 [17]. 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 [20].

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 attacks. 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 [19][22][20]. 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 [22]. 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 [4]. Hakamaki and Palomaki discuss a number of existing RFID attacks that still exist in modern RFID readers [9].

4 Research Design & Methodology

Words

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

The testing performed against the readers would be broken into three primary categories: Bluetooth, RFID, and Wiegand. These categories will follow logical attack chains to test a variety of vulnerabilites.

The Bluetooth procedures follow a primary attack chain to test for vulnerabilities. The chain starts with either gattacker [11] [15] or CrackLE [25] to gain an initial foothold. From there, the next step is to test for either injection attacks or injection free attacks [22] to clear the binding list. After the binding list is cleared a man-in-the-middle attack can be attempted [14] [17] [15]. From this point there are multiple attacks that can be attempted. The first attack is to attempt to break the long-term key by brute forcing the term key [23] [21]. After this replay attacks and active sniffing can be attempted [6] [17]. Finally, the protocol could be reverse engineered to try and find vulnerabilities in the implementation.

The primary RFID attack is cloning, it is possible to try to prevent cloning though it is very hard [3] [24] [16] [7]. Secondly, the random number generator used for RFID cards can be tested for vulnerabilities [5] [16]. A third possible set of attacks is to try passive and active relay against the reader [10] [12]. Another possibility is to examine the RFID card reader for possible injection attacks and remote code execution [8]. The final attack method would be to attack the RFID chain of trust used in the reader [13].

The Wiegand protocol attacks are relatively simple. The first step of the attack chain is to analyze the various Wiegand outputs of the reader. After a large enough scans have been made interception and duplication attacks can be made [4]. Finally, a BLEKey [2] or similar device can be made and tested against the reader. As a part of the Wiegand testing, attacks against the optical tamper sensor will need to be created and tested.

These three sets of attacks will cover a large amount of the reader's attack surface. The particular kill chains are ordered to effectively build off of previous steps and to test the easier attacks before the more complicated ones. The order also is set so that the possible dangerous attacks that could damage the device are run last.

4.3 Timeline

The timeline for this project assumes a eight week period for testing. This eight week period will be broken up into five separate stages for setup, testing, and wrapup. Eight weeks should be more than adequate to perform the necessary testing and provide a complete report. The first period is one week long and dedicated to setup. During this time a test lab would be built with the necessary equipment to test RFID, Bluetooth, and Wiegand. The second period is two weeks in length and dedicated to testing RFID. The third period is also two weeks in length, this is dedicated to testing for Bluetooth weaknesses. The fourth period is the final two week period, this time dedicated to testing for Wiegand vulnerabilities. The fifth and final period is one week in length, unlike the others this period is not for testing. The last period is dedicated to writing the report to submit to Carrier for their review.

5 Preliminary Suppositions & Implications

Words

5.1 Theoretical Implications

Words

5.2 Practical Implications

Words

6 Expected Outcomes

Words

7 Conclusions

Words

8 Acknowledgements

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

9 References

[1]

[2] M. Baseggio and E. Evenchick. Breaking Access Controls with BLEKey, 2015.

[3] K. Bu, M. Weng, Y. Zheng, B. Xiao, and X. Liu. You can clone but you cannot hide: A survey of clone prevention and detection for rfid. *IEEE Communications Surveys Tutorials*, 19(3):1682–1700, thirdquarter 2017.

[4] B. Chung. Wiegand Protocol Access: A Decade of Decryption, 2017.

[5] N. T. Courtois, D. Hulme, K. Hussain, J. A. Gawinecki, and M. Grajek. On bad randomness and cloning of contactless payment and building smart cards. In *2013 IEEE Security and Privacy Workshops*, pages 105–110, 2013.

[6] D. Filizzola, S. Fraser, and N. Samsonau. Security Analysis of Bluetooth Technology, 2018.

[7] 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)*, pages 30–35, 2017.

[8] F. Garcia, G. de Koning Gans, R. Verdult, and M. Meriac. Dismantling iclass and iclass elite, 2012.

[9] T. Hakamaki and H. Palomaki. Security of rfid-base technology, 2015.

[10] G. P. Hancke, K. Mayes, and K. Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers & Security*, 28(7):615–627, 2009.

[11] S. Jasek. Gattacking bluetooth smart devices. In *Blackhat 2016*, 2016.

[12] T. Korak and M. Hutter. On the power of active relay attacks using custom-made proxies. In *2014 IEEE International Conference on RFID (IEEE RFID)*, pages 126–133, 2014.

[13] M. Lehtonen, F. Michahelles, and E. Fleisch. Trust and security in rfid-based product authentication systems, 2007.

[14] A. M. Lonzetta, P. Cope, J. Campbell, B. J. Mohd, and T. Hayajneh. Security vulnerabilities in bluetooth technology as used in iot. *Journal of Sensor and Actuator Networks*, 7(3):28, 2018.

[15] T. Melamend. An active man-in-the-middle attack on bluetooth smart devices, 2018.

[16] A. Mitrokotsa, M. Rieback, and A. Tanenbaum. Classifying rfid attacks and defense, 2009.

[17] H. O'sullivan. Security vulnerabilities of bluetooth low energy technology (ble).

[18] C. Robberts and J. Toft. Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks, 2019.

[19] 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)*, pages 2559–2563, 2018.

[20] M. Ryan. Bluetooth: With low energy comes low security, 2013.

[21] M. Ryan. Bluetooth: With low energy comes low security. In *Presented as part of the 7th USENIX Workshop on Offensive Technologies*, Washington, D.C., 2013. USENIX.

[22] A. C. T. Santos, J. L. S. Filho, A. I. S. Silva, V. Nigam, and I. E. Fonseca. Ble injection-free attack: A novel attack on bluetooth low energy devices, 2019.

[23] S. Sevier and A. Tekeoglu. Analyzing the Security of Bluetooth Low Energy, 2019.

[24] R. van Dijk, L. Sangers, and A. Davis. Portable rfid bumping device, Feb 2016.

[25] T. Willingham, C. Henderson, B. Kiel, M. S. Haque, and T. Atkison. Testing vulnerabilities in bluetooth low energy. In *Proceedings of the ACMSE 2018 Conference*, ACMSE '18, New York, NY, USA, 2018. Association for Computing Machinery.