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 4, 2020

Abstract

Keywords

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

1 Introduction

Words

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, a Bluetooth device can be mimic and fool applications into connecting to them. In Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks, Robberts and Toft utilize 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 [4].

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 [3]. Ryan notes that the underlying encryption protocol of BLE is fundamentally weak and allows for attackers to brute force the Temporary Key. That Temporary Key can be used to derive the Long Term Key and break the encryption of the protocol [5].

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 [1]. Hakamaki and Palomaki discuss a number of existing RFID attacks that still exist in modern RFID readers [2].

4 Research Design & Methodology

Words

4.1 Definitions

4.2 Data Measurement & Analysis

Words

4.3 Procedures

Words

4.4 Timeline

Words

4.5 Novel Techniques

Words

5 Preliminary Suppositions & Implications

5.1 Theoretical Implications

Words

5.2 Practical Implications

Words

6 Expected Outcomes

7 Conclusions

Words

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

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

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

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

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