Source Summaries

Quintin Walters, Joshua Niemann, Connor Leavesley,
Daniel Capps, Jacob Ruud

February 9, 2020

Contents

1 Summary 1

1.1 Security Analysis of Bluetooth Technology

1.1.1 Group Member

Quintin Walters

1.1.2 Citation

1.1.3 Main Idea

The authors detail the security methods used in Bluetooth versions 4.X, attempt to show attacks that bypass these methods, and describe ways to harden Bluetooth security against these attacks.

1.1.4 Theory

Game Theory is the primary theory being tested in this article. The authors attack various vulnerabilities in the Bluetooth protocol in order to determine methods to increase the relative security of the protocol.

1.1.5 Method

The researchers theorized and tested primary attacks against the Bluetooth security model: Active Eavesdropping and Passive Eavesdropping. Their attacks built upon the works by Da-Zhi Sun et al., Cope et a., Das et al., and Ryan. The assets used were a Raspberry Pi running Debian, an Ubertooth, TaoTronics TT-BH07 Bluetooth Headphones, a Logitech MX Master Mouse, and a Galazy S7 Edge. The authors modified existing Bluetooth utilities for their attacks and wrote some scripts of their own.

1.1.6 Findings

The authors managed to exploit their theorized vulnerabilities successfully. They found that the JustWorks authentication method used by headsets and headphones are insecure against active eavesdropping attacks with unsophisticated hardware. The researchers also discovered that, while difficult, passive eavesdropping is still successful against hardware running Bluetooth 4.1 and recommend moving to version 4.2 or greater. They also found that devices using LE Secure Connections or Secure Simple Pairings are secure against these specific attacks.

1.1.7 Future Directions

The future directions for Active Eavesdropping is to expand and cover more than JustWorks devices, this would include attacks against mice and keyboards. The next steps for Passive Easedropping is to use the extrapolated information to decrypt packets for further analysis

and to attack other devices like keyboards and medical implants, this can be used to gather sensitive information like passwords and health data. They also stated that they could combine the two attack types to inject malicious packets or modify existing ones for other attacks against the devices. Finally, they could also do research on the vulnerabilities in Bluetooth 5.0.

1.2 Extracting the Security Features Implemented in a Bluetooth LE Connection

1.2.1 Group member

Joshua Niemann

1.2.2 Citation

1.2.3 Main Idea

The authors detail the encryption and authentication standards found in the Bluetooth Low Energy Protocol, from Bluetooth 4.0 to Bluetooth 5.0. The researchers also look at several BLE devices to analyze their security models.

1.2.4 Theory

Game Theory is the primary theory being tested in this article. The authors examine various versions of the Bluetooth protocol to determine which versions have the best security measures in place. In addition, the authors analyze BLE devices in an effort to learn which devices and device manufacturers have the best security.

1.2.5 Method

The researchers found that many modern fitness trackers use older versions of Bluetooth low energy. They also found that these fitness trackers often do not enable optional features that make bluetooth much more secure. As a result, most of the encryption was trivial to decrypt. The researchers then created an app that uses the Bluetooth sniff log functionality present in the developer section in Android to extract the security features of a bluetooth low energy device.

1.2.6 Findings

The authors managed to exploit their theorized vulnerabilities successfully. They found that the JustWorks authentication method used by headsets and headphones are insecure against active eavesdropping attacks with unsophisticated hardware. The researchers also discovered that, while difficult, passive eavesdropping is still successful against hardware running Bluetooth 4.1 and recommend moving to version 4.2 or greater. They also found that devices using LE Secure Connections or Secure Simple Pairings are secure against these specific attacks.

1.2.7 Future Directions

The authors want to make their app much more usable to the average consumer. Right now it's very oriented toward technical-minded researchers.

1.3 Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks

1.3.1 Group Member

Connor Leavesley

1.3.2 Citation

1.3.3 Main Idea

The authors outline how to approach attacking Bluetooth locks. They use well documented attacks to discover vulnerabilities in a Bluetooth low energy lock.

1.3.4 Theory

Game theory is being utilized to test the security of the lock and see where the vulnerabilities in the lock lie.

1.3.5 Method

The authors create a threat rating system following the DREAD model is to accurately represent the threat of the lock being successfully attacked. They make three threat models: unauthorized lock access, avoidance of logging, and denial of service. They use a Bluetooth man in the middle attack to gather information about the lock's Generic Attribute Profile (GATT), how the application connected to the lock, hosted services, and other characteristics of the lock. Using the GATT, an attacker could use a fake lock hosted on a Arduino board to connect to the application, and then forward all information to the actual lock. Next, the authors test access permission edge cases to see when access could be abused by an attacker to bypass controls. The authors then reversed the app to gather further insight on how the app connected to the lock.

1.3.6 Findings

Not much was able to be done in the way of breaking into the lock. Some patterns were found in the communication scheme, but nothing to indicate how the application was encrypting the connection. The authors lauched a replay attack, but this was ineffective. Fuzzing was similarly ineffective. If the owner of the lock granted an attacker permission to access it, disconnects their internet, and then the attacker's permission was revoked, the attacker can still access the lock. In the app, a possible encryption key for a database was found, but not pursued.

1.3.7 Future Directions

The authors would like to see a more structured method developed to analyze the security of Bluetooth devices, as many of the approaches they took were very time consuming.

1.4 Security Evaluation and Exploitation of Bluetooth Low Energy Devices

1.4.1 Group Member

Connor Leavesley

1.4.2 Citation

1.4.3 Main Idea

In his thesis, Captian Rose attemps to provide the industry with a wholistic look on the security of the low energy bluetooth protocol. He uses four different methods in an attempt to cover a wide range of conigurations and scenarios to really put this protocol to the test.

1.4.4 Theory

Game Theory is the primary theory being tested in this article. Captain Rose proposes multiple different scenarios where the bluetooth protocol is vulnerable in order to better understand how to secure it in the future.

1.4.5 Method

Captain Rose and his supporters used multiple different methods to test the strength and security of the Bluetooth protocol. First, he used a benchmark open-source range-finding tool to determine the location of Bluetooth devices through a novel distance estimation method, increasing the state-of-the-art device location distance from 50 meters up to 1,000 meters. Second, he evaluated 17 individual Bluetooth Low Energy devices for vulnerabilities in their operating system. Thirdly, he used user behavior analytics to demonstrate how malicious actors can exploit vulnerabilities for unauthorized device access and obtain sensitive information

1.4.6 Findings

Captain Rose's research revealed that 13 out of 17 (75 percent) of the tested devices contained at least one vulnerability resulting in unauthorized access. However, he did find that countermeasures to BLE attacks already exist and most require minimum implementation and development by manufacturers. More complex mediation techniques exist for issues that are not solved by the initial mediation techniques.

1.4.7 Future Directions

Since Captain Rose's work was done on an outdated bluetooth protocol (4.1) he mentions that there is room for others or himself to do research on devices implementing the newest protocol. He also recommends research into newly release bluetooth devices such as Lockitron or Schlage. He also states that he did not do any work with the firmware of the devices he tested so there is room for others to continue his work there. Along with that, he states that no research was done on attempting to clone the devices that he was testing, so there is more work to be done there.

1.5 Security Vulnerabilities in Bluetooth Technology as used in IoT

1.5.1 Group Member

Daniel Capps

1.5.2 Citation

1.5.3 Main Idea

This study is about understanding Bluetooth and Iot(Internet of Things) devices. They go in depth on the importance of understanding Bluetooth, the differet attacks possible against Bluetooth and IoT devices, and how to mitigate these attacks using different tequniques.

1.5.4 Theory

Game Theory is the primary theory being used in this article. The authors gathered information about many vulnerabilities and exploits in Bluetooth/Iot and determined different mitigation tequniques for each of them.

1.5.5 Method

The researchers explained the inner workings of IoT and Bluetooth and then gathered different information on attacks to Bluetooth and Iot. Then, by using the information they found they determined different risk mitigation tequniques for users of Bluetooth and IoT devices.

1.5.6 Findings

The authors presented multiple vulnerabilities and attacks against Bluetooth and IoT and risk mitigations to combat them, the most notable of them being more awareness from the user's perspective on security issue with bluetooth. The main attacks showcased here are PIN Cracking, Man-in-the-M(MITM), BlueJacking, BlueBorne, Fuzzing, Reflection/Relay, Backdoor, Denial of Service(DOS). Many more attacks are mention as well.

1.5.7 Future Directions

Can the analysis tequniques use here be used for any other wireless standard? Could there be an attack on BLE that has to do with power consumtion? What methods can we use to more properly inform users of the risks of IoT and Bluetooth so that they may mitigate said risks?

2 Summary 2

¡¡¡¡¡¡¡ HEAD

2.1 Analyzing the Security of Bluetooth Low Energy

=======

2.2 Wiegand Protocol Access: A Decade of Decryption

¿¿¿¿¿¿¿ fd5a204edbeeca30d66e6c7ca98e09b852ccfaa4

2.2.1 Group Member

Connor Leavesley

2.2.2 Citation

2.2.3 Main Idea

The authors aim to explain how Bluetooth LE protocol works and the cryptographic weaknesses in the protocol.

2.2.4 Theory

This paper is applying Game Theory. A successful cryptographic attack is a loss for the security of the protocol.

2.2.5 Method

The authors first sniffed the Bluetooth traffic with a Ubertooth using the BlueZ Bluetooth driver and associated Ubertooth drivers. Using the Blueooth handshake, the authors used Crackle to crack the Temporary Key due to its restricted key space. The Temporary Key was then used to gain access to the Long Term Key (LTK). The LTK was then used to decrypt any future communication traffic in Wireshark.

2.2.6 Findings

The authors found that the keyspace of the Temporary Key is very restricted, allowing for a very quick brute force attack. They also found that Bluetooth Low Energy was susceptible to a number of attacks due to the low power requirements: denial of service and replay attacks. It was also found that Ubertooth struggled to capture a complete pairing event. The authors suggest that the Ubertooth should be as close as possible to the source transceiver to mitigate this issue.

2.2.7 Future Directions

Many vendors likely do not implement the Bluetooth stack correctly. These vendors may also use the same stack across multiple devices. Areas of further research should focus on individual devices from the same vendor to attempt to find vulnerabilities that affect entire product lines.

2.3 Wiegand Protocol Access: A Decade of Decryption

2.3.1 Group Member

Quintin Walters

2.3.2 Citation

2.3.3 Main Idea

Brandon Chung covers what the Wiegand Protocol is, the historic vulnerabilities and hacks, what vulnerabilities still exist, and how to protect yourself against them. He spends a large amount of time on the historic attacks because most of them are still applicable, the protocol has not been hardened against them and as a result it is still very easy to exploit.

2.3.4 Theory

Chung applies Game Theory in his work, he treats the security of the Wiegand Protocol as a zero sum game in which any method of bypass is a loss for the defenders. He highlights historic vulnerabilities of the protocol that are still in existence to reinforce this belief.

2.3.5 Method

The author primarily presents the findings of others, he does little original research of his own. However, he does use an Arduino device to attack an unnamed Wiegand RFID reader. He connects his Arduino device to the Wiegand DATA 0 and DATA 1 wires, then he uses monkeyboard's "Wiegand Protocol Library for Arduino" to verify that the inherent vulnerabilities in the protocol still exist. Chung provides instructions and sample code for readers to attempt this on their own devices. This attack is the basis of the attacks done by Bernard Mehl (2015) and Zac Franken (2007), two attacks that Chung wrote in depth about.

2.3.6 Findings

Brandon Chung found that Wiegand devices are still vulnerable to decade old attacks. These attacks have been extensively documented and Chung duplicated the early stages of them to prove that they would still work. Using an arduino device, or similar microcontroller, 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.

2.3.7 Future Directions

Chung lays out multiple methods for future implementation to secure Wiegand devices. He recommends that the protocol be adapted to allow for encrypted keycards and the rejection of keycards that are not properly encrypted, he also recommends that the actual readers implement hardware methods to detect when the device has been tampered with and to report that tampering immediately to the controller. Further upgrades include remote firmware detection and updates, Wiegand devices typically are not able to be updated without direct physical contact which disincentivizes updating the readers unless absolutely necessary.