Source Summaries

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

February 1, 2020

Contents

1 Security Analysis of Bluetooth Technology

1.1 Citation

Daniel Filizzola, Sean Fraser, and Nikita Samsonau. Security Analysis of Bluetooth Technology, 2018. URL `https://courses.csail.mit.edu/6.857/2018/project/Filizzola-Fraser-Samsonau-Bluetooth.pdf`

1.2 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.

1.3 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.

1.4 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.

1.5 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.

1.6 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.

2 Extracting the Security Features Implemented in a Bluetooth LE Connection

2.1 Citation

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. doi: 10.1109/BigData.2018.8622000

2.2 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.

2.3 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.

2.4 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.

2.5 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.

2.6 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.

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

3.1 Citation

Christopher Robberts and Joachim Toft. Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks, 2019. URL `https://pdfs.semanticscholar.org/3eb1/c453464f50c30b2dfb2aff705d45bfe7a6d1.pdf`

3.2 Main Idea

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

3.3 Theory

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

3.4 Method

A threat rating system following the DREAD model is created to accurately represent the threat of the lock. Three threat models were created: unauthorized lock access, avoidance of logging, and denial of service. A Bluetooth man in the middle attack is carried out to gather information about the lock's Generic Attribute Profile (GATT), how connections are formed, hosted services, and other characteristics of the lock. Using the GATT, a fake lock can be created to connect to the application, and then forward all information onto the actual lock. Next, access permission edge cases are tested to see when access can be abused to bypass controls. The app was reversed to gather further insight on how the app connected to the lock.

3.5 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 data was being encrypted. A replay attack was launched, but this was ineffective. Fuzzing was similarly ineffective. If an attacker is granted permission to access the lock, disconnects their internet, and then their permission is revoked, the attacker can still access the lock. In the app, a possible encryption key for a database was found, but not pursued.

3.6 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.

4 Bibliography

Daniel Filizzola, Sean Fraser, and Nikita Samsonau. Security Analysis of Bluetooth Technology, 2018. URL `https://courses.csail.mit.edu/6.857/2018/project/Filizzola-Fraser-Samsonau-Bluetooth.pdf`.

Christopher Robberts and Joachim Toft. Finding Vulnerabilities in IoT Devices: Ethical Hacking of Electronic Locks, 2019. URL `https://pdfs.semanticscholar.org/3eb1/c453464f50c30b2dfb2aff705d45bfe7a6d1.pdf`.

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. doi: 10.1109/BigData.2018.8622000.