Source Summaries

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

January 30, 2020

Contents

1 Filizzola 2018 Security

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

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, Dec 2018. doi: 10.1109/BigData.2018.8622000

2.1 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.

2.2 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.

2.3 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.

2.4 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.

2.5 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 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`.

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, Dec 2018. doi: 10.1109/BigData.2018.8622000.