Hacking Electronic Internet Connected Shifters

Thomas Hansen
UW Madison

Tolga Beser
UW Madison

Chang-yen (Cody) Tsen
UW Madison

Abstract

1 Introduction

Cyclists has seen the emergence of wireless shifting technologies over the past few years. While the technology existed as far back as the 1990s, adoption has accelerated in recent years, especially for high-end bikes. As we see the technology improve, these shifters have become faster and more precise than mechanical shifting, accelerating their adoption among riders.

The wireless shifters use an assortment of communication technologies known as Personal Area Networks (PAN's) such as Bluetooth. The use of these technologies opens the once closed off bicycle to security vulnerabilities. If an attacker can trigger extraneous shifts the cyclist can be thrown off their bike causing personal injury and the potential for even larger accidents (cyclists in pro races are tightly packed causing crashes to spread quickly). While security research focused on these electronic shifters is sparse there exists a plethora of work exploring security for various Personal Area Network enabled devices. A subset of wireless shifters utilizes Bluetooth as a communication protocol which has been shown to have security flaws in several implementations. One of the wireless shifting devices that we would like to examine is the SRAM eTAP system which utilizes their novel Airea Personal Area Network protocol which allows their components to communicate from up to a hundred meters away. This large distance could allow an attacker to communicate with their components from an unobservable location.

2 Related Work

There has been a lot of work into researching how to break wireless networks on embedded electronic devices, especially those where security is not the strong suit. Many simply use replay attacks and exploit design flaws with device authentication [**?**]. Other paper look broadly on the state of wireless security, and analyse methods surrounding IoT devices and wireless communication methods [**?**] [**?**].

We attempted to take many of these findings and bring them to the electronic shifting space, and see what sorts of vulnerabilities we could find. To the best of our knowledge, no comprehensive research yet has existed on the security wireless shifters for bikes. We studied the Archer Components DX1, SRAM eTap, and Shimano Di2 for vulnerabilities.

3 Potential Impact

Electronic shifters in bikes have become extremely popular among high-end bikes. Tadej Pogačar, the overall winner of the 2021 and 2020 tour won using a Campagnolo EPS shifter. Egan Bernal, the 2019 winner, won riding a Pinarello that used Shimano Dura Ace Di2 shifters [**?**]. Furthermore high-end bikes, such as the Trek Madone 9, are sold by defualt with electronic shifters.

Competitions furthermore have high stakes. The Tour de France prize pool is 3.6 million AU, and many millions stand to be gained from partnerships and sponsors. Anyone who's able to impact a race in their favor may realize substantial financial gain, and we only expect the potential professional impact to expand with time.

Lastly is the impact on line. Biking is a sport where even more casual riders will go for hours, and being able to disable a bike and strand someone somewhere can make them more vulnerable or otherwise threaten their wellbeing. It's because of all of these reasons we think the security of electronic shifters is an important topic that deserves research.

3.1 Contributions

Our major contribution to the field was bringing proper security testing to electronic sifters in the biking industry. These devices have become increasingly popular among professionals and performance cyclists, and there's no real analysis of which devices provide the best, if any, security to the biker.

Some devices, like the STRAM eTap, claim

3.2 Common Attacks Against IoT Devices

The security of IoT Devices is well documented and various devices have been studied in recent years. [cite papers here] Because the research body is so vast we will derive a few common attack vectors. The attack vectors that we will outline are Replay Attacks[cite], Denial of Service[cite], and Man in the Middle Attacks[cite].

(1) Replay Attacks are conducted by recording communication signals between IoT Devices and replaying them. Without a dynamic key(not sure if this wording is right) these false signals will be non-discernible from the legitimate commands. [cite]
(2) Denial of Service(DDOS) attacks have been shown to be effective against a variety of IoT devices. Lack of processing power among small IoT devices compounds their risks to such attacks. [cite]
(3) Man in The Middle(MITM) attacks intercept communications from IoT devices and proceed to act as the expected receiver/communicator.[cite]

3.3 Research in wireless attacks against other vehicles

4 Devices

4.1 Archer Components DX1

4.2 Shimano Di2

4.3 SRAM Force AXS

5 Security Analysis

5.1

6 Evaluation

7 Recommendations

8 Conclusions

9 Future Work