Hacking Electronic Internet Connected Shifters

Thomas Hansen
UW Madison

Tolga Beser
UW Madison

Chang-Yen Tseng
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 [4]. Other paper look broadly on the state of wireless security, and analyse methods surrounding IoT devices and wireless communication methods [3] [5].

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 [2]. 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 anal-

ysis 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 D1X

The Archer D1X is a modular electronic shifting system that can be integrated into a wide array of derailleur-shifting groupsets. While the other two components groups that we study come with custom derailleurs that are wirelessly enabled the D1X focuses on integrating into existing systems. It is installed near the derailleur with the shifting cables routing through it. This allows the D1X to change the tensions of the shifting cables and therefore the gears. The electronic shifting box is wirelessly connected to the bluetooth enabled hand shifters which allow the users to send shifting signals. Of note, the D1X is the only component that we will study that utilizes the bluetooth protocol for communication between shifter and shifting box (akwardly worded need to change).

The setup for the D1X is largely influenced by the bluetooth protocol (probably cite here). On first use, both the shifter and the shifting box need to be turned on with the power button pressed for specific lengths of time (fact check this). This allows the components to go through a one time pairing process, subsequent uses do not require this step. The user can also connect to the shifting box with their smartphone using the Archer mobile application. This is done by turning on the shifting box and going to the Archer application to pair (fact check if we press another button). Through the application the user can set shifting profiles allowing them to dictate specific gears that should be changed upon a shifting command. (Didn't want to talk about connection vulnerability here)

4.2 Shimano Di2

4.3 SRAM Force eTap AXS

The SRAM Force eTap AXS [1] is marketed toward professional, competitive bikers, and is price most premium out of all of our components. It works completely wirelessly like the Archer Components DX1, where there is no need for physical wire between the derailleur and the shifters. The SRAM is also the only one in our lineup that uses a proprietary protocol. The derailleur and the shifter communicate using the in-house AIREA protocol that operates within the 2.475Ghz frequency range. During a press event of this products, SRAM claims that the protocol uses 128-bit rolling encryption and the system is "more secure than any cash machine".[6] The system also provides Bluetooth for connecting to a smartphone and ANT+ to send information to a bicycle computer.

To set up the SRAM system, the biker will have to click a button on the derailleur to enter pairing mode and then click the buttons on both shifters consecutively to finish the pairing process. To connect to a mobile phone, the biker will start an app on their phone, select their SRAM system, and long-press a button on the derailleur to authorize. Note that the app provides ways to remap each shifter to different operations (gear up, gear down), but the user is not able to shift the gear directly in the app.

5 Security Analysis

5.1 Threat Model & Goal

We want to protect the safety of the bikers with such electronic shifters as sudden shifting when unintended may cause massive harm. We assume a scenario where bikers are joined with some malicious actors in a large-scale biking competition. In this scenario, we assume the adversary has access to the type of shifter the victim is using. The adversary can also be in close proximity with the victim before or during the competition, as a result, they can send arbitrary radio signals to the victim. We further assume the adversary can have a very short period of physical access with the victim's bike before the competition, such as when the victim is not looking.

We define a successful attack as making a victim's bike shift to an unintended gear during the competition. We assume all competitors will do a quick test ride before the competition and don't consider denial of service before the competition as a successful attack since this does not introduce safety risks to the riders. For that reason, simple attacks such as cutting the victim's breaking cable or poking a hole in the victim's tire will be trivially easy to spot during the test ride and thus won't qualify as a successful attack.

5.2 Bluetooth Pairing Weekness

5.3 SRAM Replay Attack

From the public FCC data, we know that the SRAM system's operating frequency is around 2.475GHz with a bandwidth of 3MHz, therefore, we use an SDR and the Universal Radio Hacker software[7] to analyze the signals between the shifters and the derailleur. We find out that every time the shifter is pressed, it will emit a signal continuously for about 1.2 seconds and we didn't observe any ACK-like signal from the derailleur. We further discover that recording a gearing event signal from a shifter and replaying it will cause the derailleur to act accordingly. However, the recorded packet will be invalid whenever the biker presses the same side of the shifter again. We suspect that each shifter has its own internal counter that the derailleur keep track of so it can invalidate all previous packet after receiving a new one.

However, the ability to replay the latest packet still opens up a way to attack the system. Based on the aforementioned vulnerability, we designed an algorithm specifically to attack an SRAM system during competition. We set up the SDR in a way that it will continuously switch between receiver and sender mode. During the receiver mode, the SDR will capture signals from the air and detect if it contains an SRAM gearing signal. If it does, it stores the new signal. Then it will send the saved signal (either the newly captured one or something stored before) to the air, causing the victim's bike to shift unintendedly.

Since SRAM does not release their firmware let alone source code, we do not have a reliable way to detect whether a signal segment contains an SRAM shifting packet or not. Therefore, we use a simple SVM classifier to solve the problem. We prerecorded several SRAM gearing signal segments and trained the model along with white noise and signal from other 2.4Ghz devices. In the end, we can reach 100% accuracy in a lab environment.

We setup the attack with a HackRF One SDR. Under the attack, when the victim shifts near the attacker, their derailleur will continuously shift to the highest or lowest, and even if the victim counter shift, they will find out that their system shift to the other extreme direction.

Algorithm 1 SRAM replay attack algorithm

```
saved ← None
while True do
    Set up SDR in receiver mode
    signal ← get signal from SDR for 1 second
    if signal match SRAM pattern then
        saved ← signal
        Setup SDR in sender mode
        Send saved
    end if
end while
```

Potential Optimization In the attack, if the victim happens to shift the same gear while the SDR is in sender mode, subsequent attacks will fail. However, there are possible ways to optimize this attack.

- **Use two SDRs one for receiving and one for sending.** Clearly, in this setting, the attacker will be able to notice the victim's signal while they are sending their malicious signal. However, the attacker's receiver will now be interfered by their sender, and special care needs to be done to avoid confusion.

- **Trim the saved data.** During investigation, we found out that while the signal from the shifter lasted over 1 second, 50ms worth of data is enough to cause the derailleur to act. Therefore, it is possible that we can trim the data so that the SDR can send the data and be in sender mode for just a little amount if time, greatly reducing the chance of missing the victim's signal.

6 Evaluation

7 Recommendations

8 Conclusions

9 Future Work

References

[1] etap AXS. https://www.sram.com/en/sram/road/collections/etap-axs. [Online; accessed 2021-12-01].

[2] Egan bernal's pinarello dogma f12 x light tour de france winner's pro bike, March 7 2020.

[3] CHOI, M.-K., ROSSLIN, J., ROBLES, R., HONG, C.-H., AND KIM, T.-H. Wireless network security: Vulnerabilities, threats and countermeasures. *International Journal of Multimedia and Ubiquitous Engineering 3* (08 2008).

[4] DANIEL HALPERIN, THOMAS S. HEYDT-BENJAMIN, B. R. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. *IEEE Symposium on Security and Privacy* (2008).

[5] KREJČÍ, R., HUJŇÁK, O., AND ŠVEPEŠ, M. Security survey of the iot wireless protocols. In *2017 25th Telecommunication Forum (TELFOR)* (2017), pp. 1–4.

[6] PHILLIPS, M. Sram Red eTap is a Step Forward for Electronic Shifting. *Bicycling* (aug 26 2015). [Online; accessed 2021-12-02].

[7] POHL, J., AND NOACK, A. Universal radio hacker: A suite for analyzing and attacking stateful wireless protocols. In *12th USENIX Workshop on Offensive Technologies (WOOT 18)* (Baltimore, MD, 2018), USENIX Association.