RFID Key Fobs in Vehicles: Unmasking Vulnerabilities & Strengthening Security

Devon Magda
demagd9422@ung.edu

Bryson R. Payne
University of North Georgia

RFID Key Fobs in Vehicles: Unmasking Vulnerabilities and Strengthening Security

Devon E. Magda
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, GA, USA
demagd9422@ung.edu
0009-0003-1547-9819

Bryson R. Payne
Department of Computer Science and Information Systems
University of North Georgia
Dahlonega, GA, USA
bryson.payne@ung.edu
0000-0003-4539-0308

***Abstract*— In modern vehicles, radio frequency identification (RFID) key fobs, a form of remote keyless entry (RKE), play a pivotal role in vehicular security and functionality. The goal of this research is to implement and demonstrate radio-based cyber-physical attacks against identified vulnerabilities associated with RFID key fobs and provide insights on how to fortify security precautions against such attacks. Furthermore, this research reviews and acknowledges pre-existing security features that have been implemented to prevent the recurrence of these vulnerabilities. An additional goal of this research is to discover the security disparity between RFID tags and readers from vehicles manufactured in the early 2000s and vehicles from the mid-2010s or later.**

Keywords*— *RFID (radio frequency identification), automotive security, replay attacks, rollback attack, rolljam attack, car hacking.

I. Introduction

RFID technology is relatively new to the automotive industry, starting in the late 1980s to early 2000s, first introduced in cars for remote keyless entry (RKE) and ignition. RKE fobs are small remote controls that contain an RFID chip and antenna that can interact with an RFID reader to receive power and transmit a signal back to the vehicle [1], usually to lock, unlock, and start the automobile.

Early RKE fobs were vulnerable to cloning, replay attacks, and man-in-the-middle attacks, as there were no security precautions set in place for the first several model years featuring remote keyless entry. However, the integration of basic encryption into RFID systems in the mid-2000s became an important accomplishment for heightened security and vulnerability mitigation [2]. This addition of basic encryption paves the way, allowing for a more secure utilization of RKE technology in vehicles. Additionally, the improvements in encryption techniques have deterred criminals from cloning RFID signals by hardening the RKE technology against malicious exploits. One innovative RFID security feature recently added uses a pseudo-random sequence generator that allows for a unique unlock sequence to occur after every use. The purpose of these features is to prevent carjacking from occurring, provide a more secure environment, and allow potential use of RFID systems in other applications besides vehicles.

II. Related Work

In the evolution of vehicular security, RFID technology continues to adapt and improve in response to exploits that previously occurred. Originally, remote keyless entry technology was largely insecure because of the exposure to replay attacks and lack of encryption [2]. RFID technology was still new at this stage; therefore, many individuals did not know the extent to which RFID was vulnerable. In the years since, RKE fob security has continued to improve with the introduction of encryption and rolling codes to enable a safer experience for vehicle owners.

Two main attacks are used by carjackers to gain access to vehicles by copying RKE fob signals, the RollBack attack and the RollJam attack [3]. The original replay attack [4], which proved effective on many older vehicles, involved capturing a specific frequency once and then perpetually reusing it as cars would use a static code when RFID technology first came out [1].

Although this worked on older models, this method has become obsolete with newer vehicles due to the addition of rolling codes and encryption; however, a new vulnerability in these vehicles has occurred which involves simultaneously jamming and copying the frequency enabled to unlock the vehicle. [3]. This type of attack was first discovered by Samy Kamkar and is known as a RollJam attack. This attack works by jamming the original signal sent to the vehicle and copying it at

the same time. Now, when the user sends the second unlock signal the attacker captures it and jams it again but plays the first unlock signal that was captured. Essentially, the attacker will be able to play the second unlock signal that was captured later if no other unlock signal was used afterward, therefore demonstrating a vulnerability in rolling code-based schemes [3].

There is another attack similar to this one, known as a RollBack attack, which has the same premise except the attacker lets the second signal go through without jamming it. By doing this, the attacker can replay the two unlock signals consecutively, which will grant access multiple times. This works by causing the vehicle to resynchronize with a previous code when using the first jammed code to roll back and then the second unlock signal lets the attacker in [5]. This is the basis of how the attack works; however, depending on the make, model, and year of the automobile, and the manufacturer and chip generation of the remote keyless entry (RKE) fob used in the car, some vehicles can require more than two unlock signals to be recorded and replayed to resynchronize the vehicle [3]. It should be noted that Csikor's research [3] did not list the remote keyless entry chip manufacturers by name, referring to them only as "Mfr. 1" to "Mfr. 5" for security reasons. However, industry research by Technavio notes that the top five RKE manufacturers are responsible for 65% of all remote keyless entry systems in the market [6].

The RollBack attack described above works with almost every vehicle using RKE fobs from manufacturers 1 to 3 (not identified by name, for safety reasons) as they tend to not use rolling codes or challenge-response mechanisms. The specific vulnerabilities associated with these key fobs also depend on the make, model, and year of the car as some of these vehicles have enhanced security features. Although the RollBack attacks can work on Mfrs. 1-3, some vehicles require more unlock signals to let the attacker in, and not all chips from Mfr. 1 are vulnerable [3].

Vehicles that use chips from Mfr. 4 seem to be unaffected by this RollBack attack as the different chips use rolling codes or challenge-response mechanisms which render the attacks useless [3]. Many vulnerable vehicles ultimately remain susceptible to RollBack attacks, because even if the unlock signals are copied and stored for a significant duration, such as 100 days, they still effectively unlock the vehicle, revealing that the validity of these codes does not necessarily diminish over time [7].

One device that allows for these attacks to occur successfully is the HackRF One, which can capture and send signals (*HackRF One - Great Scott Gadgets*, n.d.). The device allows attackers to be very particular as all communication signals that emit a radio frequency must be registered with the Federal Communications Commission (FCC) [3]. It is quite simple to look up the car's year, make, and model, find the corresponding key fob associated with the vehicle, and determine the FCC ID of the key fob the vehicle uses. [8].

The FCC ID provides valuable insight into a remote keyless entry fob's operational frequency by accessing the FCC's database. And, by using this information, it becomes simpler to configure tools like the HackRF for signal interception and analysis. Since this information is publicly available, this allows carjackers to determine the frequency much easier and to determine what their device needs to be tuned into when attempting to copy the unlock signals to get into a specific vehicle. Ultimately, the HackRF One is a flexible software-defined radio that can be used to issue RollJam or RollBack attacks.

III. Approach and Implementation

To properly obtain a vehicle's unlock signal from an RFID key fob, we must first use the HackRF One to obtain the signal once the key fob is pressed. The HackRF One will be used throughout this implementation to receive and transmit signals. Additionally, we are using the Universal Radio Hacker software on Windows as it seemed to be the most straightforward software that could easily receive and transmit signals without installing multiple other dependencies. We attempted to use GNU Radio Companion at first; however, there were too many issues involved to get it to function correctly.

A. Obtaining the Frequency Using FCC ID

For the first part of this implementation, we will use the website "apps.fcc.gov" and type in the FCC ID to obtain the frequency the key fob transmits (Figure 1). To find the FCC ID, you can look at the back of your key fob or look up the type of car you have along with the terms "Key Fob FCC ID" on Google. In addition, the FCC ID website also contains information related to the block diagram which allows us to see information about the transmitter. Since we located the FCC ID, we now have information corresponding to the frequency that the HackRF One can listen on. We can now boot up the next software that will be used called Universal Radio Hacker.

FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
:OUCG8D-399H-A	Original Equipment	01/30/2004	313.85	313.85

Fig. 1. The FCC ID and frequency on which the key fob operates.

B. Unlocking the Vehicle by Tuning into the Frequency

The Universal Radio Hacker and HackRF One will be collaboratively utilized to seamlessly intercept signals from the key fob and responsively transmit signals back to the vehicle. First, the spectrum analyzer must be started in Universal Radio Hacker as this will allow us to tune in to the exact frequency the device is operating on (Figure 2). At this point, we were able to tune in to the frequency of 313.85MHz, and the spectrum analyzer allows you to fine-tune the frequency it needs to record. After this, we clicked on the Record Signal button and since we used the spectrum analyzer last, it allowed the frequency to be carried over to when we started to record the signal.

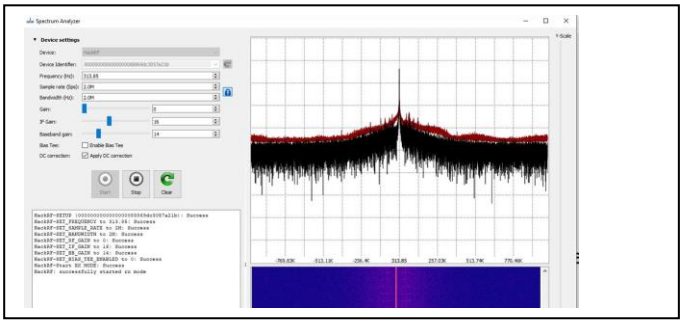
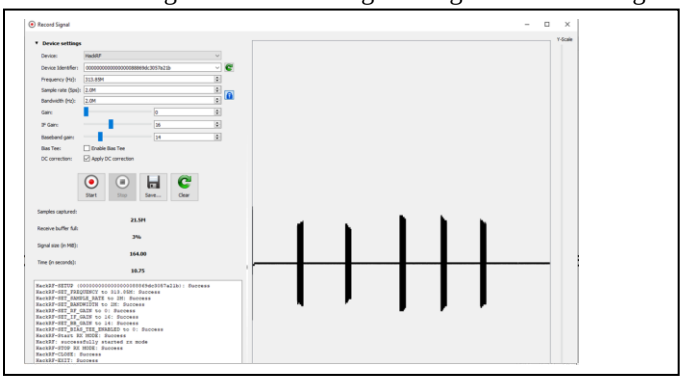


Fig. 2. The spectrum analyzer in Universal Radio Hacker tuned into the frequency recovered from the FCC ID.

Now that the signal is being recorded, we pressed the unlock signal on our key fob 5 times with an interval of around 2 seconds in between each click (Figure 3). After this, all we have to do is press the play button on Universal Radio Hacker, and this transmits the signal back through the HackRF One and allows it to unlock the vehicle (Figure 4). In our experiment, we were able to unlock a 2010 Honda Odyssey; however, we had to let the first 4 signals we recorded go through until the 5th signal



was able to unlock the vehicle. We also attempted the same method with another vehicle owned by one of the authors, a 2003 Honda Accord, and this vehicle was also unlocked once we let the first 4 signals go through. Not only that, we recorded a new set of unlock signals for the 2010 Honda Odyssey. We discovered that after replaying the first 4 unlock codes we had captured, any subsequent codes that came after ended up unlocking the vehicle.

Fig. 3. This figure shows the result of recording the signal in Universal Radio Hacker as the key fob is pressed.

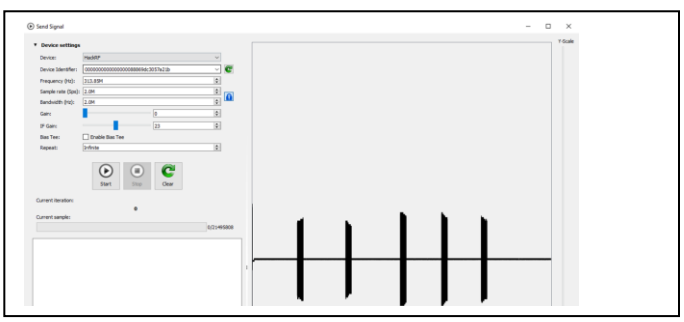


Fig. 4. Sending the signal from Universal Radio Hacker using the HackRF One to attempt to unlock the vehicle.

IV. Results

After many attempts and finding software that satisfies the requirement to receive and transmit signals, we were able to successfully hack a 2010 Honda Odyssey and a 2003 Honda Accord. We were able to determine that the 2010 Honda Odyssey RFID key fob transmits the unlock and lock signals on 313.85MHz. Interestingly enough, we did another test with a frequency of 315MHz and discovered that recording and transmitting the signal on this frequency also worked. Although this vehicle is secure from a simple replay attack, which involves just copying an unlock code and transmitting it back to the vehicle, it is still vulnerable to both RollBack and RollJam attacks. We were able to successfully use a RollBack attack to get into the 2010 Honda Odyssey. Unfortunately, we had no way to jam the signal to attempt a RollJam attack; however, those attacks do not let an attacker into the vehicle multiple times like RollBack attacks do. Upon further testing, we were able to discern that the 2010 Honda Odyssey and the 2003 Honda Accord require the same number of unlock codes (4) to roll back the vehicle, and then any codes after will unlock the vehicles.

At first search, we were unable to determine the exact information regarding the manufacturers and chips that were used for the 2010 Honda Odyssey and 2003 Honda Accord; however, we can determine that the chipsets are similar since both required the same number of unlock codes to roll back the vehicles before we could successfully unlock them. Using the FCC ID search later, we discovered that both RFID key fobs from the vehicles are manufactured by the NEC Corporation with the same CPU type UPD789860 [9,10]. By looking at the user manual RFID key fobs for both vehicles, it is interesting to see that both of the CPUs have the same information, which would explain why both vehicles require the same number of codes before they unlock.

Fig. 5. Implementing the RollBack attack in the demonstration video linked in our presentation.

As a result of utilizing the HackRF One and Universal Radio Hacker, we have successfully gained access to the 2010 Honda Odyssey using unlock signals as we can see in the video (Figure 5). In the next video, we demonstrate that once the first set of unlock codes successfully bypasses the security using a RollBack attack, any subsequent recorded codes can also unlock the vehicle (Figure 6). Unfortunately, whenever the key fob is

pressed again, the RollBack attack must occur again for all the subsequent recorded codes to unlock the vehicle.

Fig. 6. Using recorded codes after the RollBack attack to successfully unlock the vehicle.

As a result of the RollBack attacks, we can determine that Honda Vehicles before the year 2003 up to 2010 are vulnerable to infiltration even though they have rolling codes. Ultimately, this attack is possible if you have access to someone's RKE fob; however, it is unknown how many unlock signals an attacker would have to copy to gain access to different types of vehicles.

V. CONCLUSIONS AND FUTURE WORK

This research set out to explore the security implications associated with RFID technology in vehicles, with a focus on unmasking vulnerabilities that coincide with the technology. During this project, we discovered how to use the HackRF One to capture and transmit signals by understanding the intricacies of RFID technology associated with the key fob and the vehicle. Although RFID technology has achieved security advancements, there are still vulnerabilities that allow for RollBack attacks and RollJam attacks to occur and compromise vehicle integrity.

These attacks highlight the need for continuous security implementation as these attacks will continue to occur unless car manufacturers decide to allocate more resources to understanding how these vehicles can be compromised with all the new technology coming out. It is interesting to see how security has evolved as many vehicles could be compromised in the '90s and early 2000s due to the use of static codes which only required someone to copy the signal once to have permanent access to that vehicle.

RFID technology has since adapted from static codes and now uses rolling codes, encryption, advanced modulation schemes, mutual authentication processes, and more to improve security. Unfortunately, it is difficult to determine exactly what vehicles would be vulnerable to a RollBack and RollJam attack without all the necessary information as not every company uses the same remote keyless entry fob manufacturer. Not only that, the readers in the vehicle that communicate with the key fob are also made by different companies which can impact the ability to allow RollBack or RollJam attacks to occur.

Essentially, these attacks come down to the vulnerabilities in the key fob, the security mechanisms in the RFID reader of the vehicle, and the communication protocol that is used between the two. Manufacturers of each device, system, and automobile must work together and put every effort into vehicle security, including penetration testing of their vehicles and systems, to prevent such attacks from occurring.

Finally, there is a future for professionals interested in automotive cybersecurity, as it is critical for people to feel safe and not have to worry about their cars being stolen. The potential vulnerabilities associated with vehicles are quite alarming and could lead to an increase in vehicle theft if people were to understand how easy it is to implement such attacks. As technological advancements continue to occur, we must continue to harden systems and fortify security measures so that people can feel safe and not have to worry if somebody will steal the radio transmissions that allow access to their cars.

Overall, security should remain a primary focus for automotive companies and equipment manufacturers to ensure the safety and peace of mind of individuals who choose to buy vehicles that feature remote keyless entry.

REFERENCES

[1] C. Smith. *The Car Hacker's Handbook: A Guide for the Penetration Tester*. 2016. San Francisco, No Starch Press. ISBN: 978-1-59327-703-1. http://docs.alexomar.com/biblioteca/thecarhackershandbook.pdf

[2] F. Thornton, C. Lanthem. *RFID security.* Syngress, 2006.

[3] L. Csikor, H. W. Lim, J. W. Wong, S. Ramesh, R. P. Parameswarath, M. C. Chan. RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems. 2022. *arXiv e-prints* (2022): arXiv-2210. https://doi.org/10.48550/arXiv.2210.11923

[4] B.R. Payne. Car hacking: Accessing and exploiting the can bus protocol. *Journal of Cybersecurity Education, Research and Practice* 2019, no. 1 (2019): 5. https://digitalcommons.kennesaw.edu/jcerp/vol2019/iss1/5/

[5] L. Csikor. RollBack - Part I. - Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems. (2022a). Youtube. https://www.youtube.com/watch?v=auPtxnbly4s&t=13s

[6] Technavio. Automotive Remote Keyless Entry System Market by Vehicle Type, End-user, and Geography - Forecast and Analysis 2022-2026. Technavio. September 2022. 160 pages. https://www.technavio.com/report/automotive-remote-keyless-entry-system-market-industry-analysis

[7] L. Csikor. RollBack - Part II/A. - Mazda after 3 months. (2022b). Youtube. https://www.youtube.com/watch?v=ItY11yo95R8

[8] J. Chambers. Use HackRF SDR to Lock / Unlock a Car. James A. Chambers. August 15, 2022. https://jamesachambers.com/use-hackrf-sdr-to-lock-unlock-car/

[9] FCC. OET List Exhibits Report. February 13, 2002. https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&calledFromFrame=N&application_id=luTdy6PAHhSLX9Ik1frqZA%3D%3D&fcc_id=OUCG8D-380H-A

[10] FCC. OET List Exhibits Report. January 30, 2004. https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&calledFromFrame=N&application_id=689ZHDyzhR%2BMU5p%2FAZDbzQ%3D%3D&fcc_id=OUCG8D-399H-A