UNG | UNIVERSITY of NORTH GEORGIA™

RFID Key Fobs in Vehicles: Unmasking Vulnerabilities & Strengthening Security

Created By: Devon Magda

What is RFID Technology?

- RFID technology is relatively new to the automotive industry starting in the late 1980s and early 2000s becoming first introduced in cars for keyless entry and ignition.
- Key fobs are little remote controls that contain an RFID chip and antennae which can interact with a RFID reader to receive power and transmit a signal back to the vehicle (Smith, 2016).

History & Evolution of RFID in Cars

- The original key fobs were vulnerable to cloning and man-in-the-middle attacks as RFID is susceptible as there were no secure security implications set in place at the time. However, the integration of basic encryption into RFID systems in the mid-2000s became a huge accomplishment for heightened security and vulnerability mitigation (Thornton & Lanthem, 2009).
- The addition of basic encryption paves the way, allowing for a more secure utilization of RFID technology in vehicles.

Recent Innovations in RFID Security

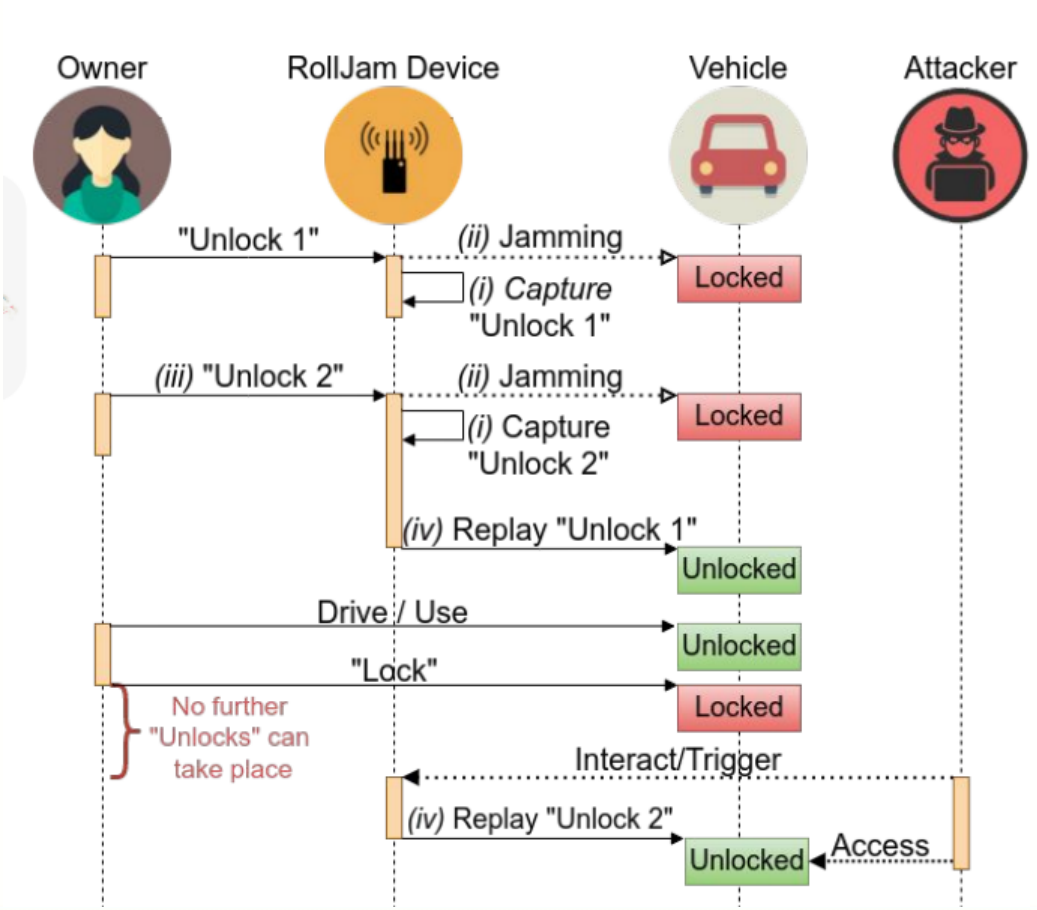
- One innovative RFID security feature recently added uses a pseudo-random sequence generator that allows for a unique unlock sequence to occur after every use.
- The overall purpose of these features is to prevent carjacking from occurring, provide a more secure environment, and to allow for the potential of RFID use to occur in other areas besides vehicles.

Initial Vulnerabilities & Replay Attacks

- The original replay attack, 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 (Smith, 2016).
- Although this worked on older models, this method has become obsolete with the newer vehicles due to the addition of rolling codes and encryption

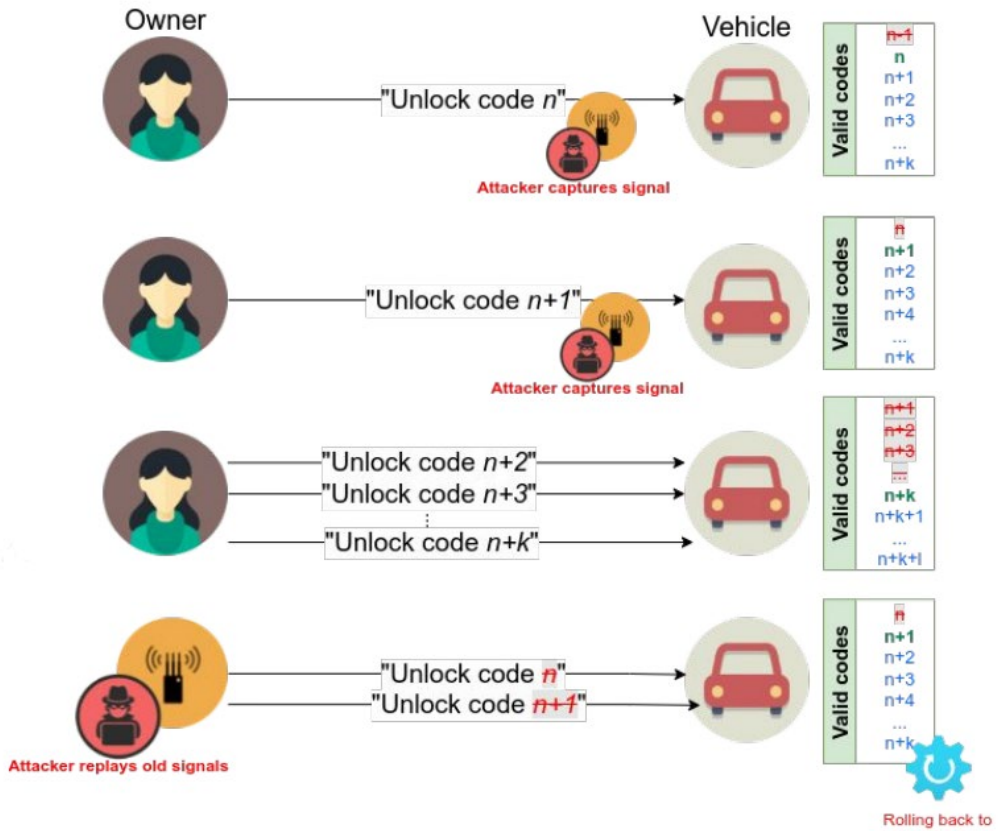
RollJam Attacks

- A new vulnerability in these vehicles has occurred which involves simultaneously jamming and copying the frequency enabled to unlock the vehicle. (Csikor et al., 2022).
- This type of attack was first discovered by Samy Kamkar and is known as a RollJam attack.



RollBack Attacks

- There's another attack similar to RollJam attacks 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 (Csikor, 2022a).



MFR & Vulnerabilities

- The RollBack attack listed above works with almost every vehicle using Manufactured Restricted key fobs (MFR) 1 to 3 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.
- Vehicles that use 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.

Car Make	Model	Mfg. date	RKE manufacturer	RollBack (variant)
Honda	Model 1 (hybrid)	2016	Mfr. 1 - chip 1	$RollBack_{\otimes}^{Strict}(5)$
	Model 1	2018	Mfr. 1 - chip 2	$RollBack_{\otimes}^{Strict}(5)$
	Model 2	2017	Mfr. 1 - chip 1	$RollBack_{\otimes}^{Strict}(5)$
	Model 3	2017	Mrf. 1 - chip 1	$RollBack_{\otimes}^{Strict}(5)$
Hyundai	Model 1	2015	Mfr. 2 - chip 1	$RollBack_{\otimes}^{Loose}(2)$
	Model 1	2012	Mfr. 1 - chip 3	NO
	Model 2	2020		NO
Kia	Model 1	2017	Mfr. 2 - chip 2	$RollBack_{\otimes}^{Loose}(2)$
	Model 1	2015	Mfr. 2 - chip 2	$RollBack_{\otimes}^{Loose}(2)$
Mazda	Model 1	2018	Mfr. 1 - chip 4	$RollBack_{\otimes}^{Strict}(3)$
	Model 2	2018	Mfr. 1 - chip 5	$RollBack_{\otimes}^{Strict}(3)$
	Model 3	2020	Mfr. 1 - chip 4	$RollBack_{\otimes}^{Strict}(3)$
	Model 4	2019	Mfr. 1 - chip 4	$RollBack_{\otimes}^{Strict}(3)$
	Model 5	2018	Mfr. 1 - chip 5	$RollBack_{\otimes}^{Strict}(3)$
Nissan	Model 1	2014	Mfr. 1 - chip 6	NO
	Model 2	2009	Mfr. 3 - chip 1	$RollBack_{5}^{Strict}(2)$
	Model 3		Mfr. 1 - chip 7	$RollBack_{8}^{Strict}(2)$
Toyota	Model 1			NO
	Model 2		Mfr. 4 - chip 1	NO
	Model 3		Mfr. 4 - chip 2	NO

The Role of HackRF One

- The HackRF One can capture and send signals
- The HackRF One allows attackers to be very particular as all communication signals that emit a radio frequency must be registered with the Federal Communications Commission (FCC) (Csikor et al., 2022).
- Essentially, you can look up the FCC ID of the key fob and determine the frequency it operates on.
- The FCC ID provides valuable insight into a key 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.

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

UNG
UNIVERSITY of NORTH GEORGIA™

Implementation (RollBack Attack)

UNG
UNIVERSITY of NORTH GEORGIA™

Implementation (RollBack Attack Pt. 2)

UNG
UNIVERSITY of NORTH GEORGIA™

Conclusion

- RFID technology has since adapted from static codes and now use rolling codes, encryption, advanced modulation schemes, mutual authentication processes, and more in order to improve security.
- Unfortunately, it's 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 MFR's.
- As technological advancements continue to occur, it's important that we continue to fortify security measures so that people can feel safe and not have to worry if somebody will steal the radio transmissions that allow for access to their car.

References

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

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

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

Csikor, L., Lim, H., Wong, J., Ramesh, S., Poolat Parameswarath, R., & Chan, M. (2022). *RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems*. https://arxiv.org/pdf/2210.11923.pdf

HackRF One - Great Scott Gadgets. (n.d.). Great Scott Gadgets. Retrieved June 24, 2023, from https://greatscottgadgets.com/hackrf/one/

Office, F. (2002, February 13). *OET List Exhibits Report*. Fcc.gov. https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&application_id=luTdy6PAHhSLX9Ik1frqZA%3D%3D&fcc_id=OUCG8D-380H-A

Office, F. (2004, January 30). *OET List Exhibits Report*. Fcc.gov. https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&application_id=689ZHDyzhR%2BMU5p%2FAZDbzQ%3D%3D&fcc_id=OUCG8D-399H-A

Smith, C. (2016). *The Car hacker's handbook : A Guide for the Penetration Tester*. San Francisco No Starch Press. http://docs.alexomar.com/biblioteca/thecarhackershandbook.pdf

Thornton, F., & Lanthem, C. (2009). *RFID Security*. Newnes. https://ebookcentral.proquest.com/lib/northgeorgia/reader.action?docID=256368

https://apps.fcc.gov/oetcf/eas/reports/ViewExhibitReport.cfm?mode=Exhibits&RequestTimeout=500&calledFromFrame=N&application_id=luTdy6PAHhSLX9Ik1frqZA%3D%3D&fcc_id=OUCG8D-380H-A