Replay Guardian: Unleashing Real-Time Car Access Without Keys

A Proposal to:

Dr. Luis Antonio Garcia

as part of

CYBER-PHYSICAL SYSTEMS (CPS) AND INTERNET-OF-THINGS (IOT) SECURITY (CS 6963) - Fall 2023

Team Members:

1. Name: Sakshi Singh

UID: u1418696

2. Name: Md Raihan Ahmed

UID: u1374605

3. Name: Ganesh Jayantrao Dharmadhikari

UID: u1471994

Need:

Problem Statement: The RollBack attack can unlock vehicles by replaying captured key fob signals, representing a significant security threat. Effective countermeasures against RollBack need to be developed and evaluated.

Remote Keyless Entry has evolved to be like magic wands for cars. Keyless entry systems, we call it a modern charm allowing you to lock and unlock your car without physically inserting a key. These systems send secret codes to your car each time you press the button on your car key. However, there's a sneaky trick known as RollJam that can mess with these systems. It involves blocking the secret codes from reaching your car, reading those codes, stealing those, and then using those later to unlock your car without your presence. The good news is that RollJam only works if the thief keeps using it. If you use your regular car key once, the stolen codes won't work anymore. So, while RKE systems are convenient, knowing these potential tricks is essential to keeping your car safe.

Significance: The development of rollback attacks is significant as it highlights vulnerabilities in security systems, particularly in the context of Remote Keyless Entry (RKE) for cars. These attacks reveal potential weaknesses that could be exploited by hackers, emphasizing the need for improved security measures to protect users and their vehicles. Some car keys has weak encryption methods. This makes it easier for hackers to break in. It is important to understand these vulnerabilities for developing stronger security protocols. In this way, car manufacturers can ensure the safety and privacy of users' assets. According to the researchers [1], rollback affects 70% of vehicles and enables unauthorized access and theft. Mitigating this widespread attack is crucial for vehicle security.

Challenges: When it comes to the security of car keys, there are a few big challenges:

1. Rolling Codes: Imagine your car key fob has a secret code, that changes every time you use it. The complexity lies in attempting to record and reuse these constantly changing codes to deceive your car into unlocking.

2. Signal Snatching: Intercepting the signals emitted by your car key when you press its buttons poses a formidable challenge. These intercepted signals can later be utilized to unlock your car. Additionally, employing devices to mislead your car into perceiving your key as nearby, even when it's not physically close, presents a challenge.

3. Cloning: Creating a copy of your car key signals by surreptitiously replicating its codes without your knowledge is a task demanding a high level of skill and sophistication. This essentially produces a duplicate key, all while remaining undetected.

Approach:

Imagine having a special key for your car that transmits a secret code every time you use it to lock or unlock your car. Which is adding an extra layer of security. However, out technique called RollBack poses a threat. RollBack involves recording instances when you use your key and playing these recordings sequentially. This confuses the unique code system in your car, reverting it to an older code known to the attacker. Consequently, they can use your car key to unlock your car without raising suspicion. In essence, RollBack is a clever way for malicious individuals to access your car, even with a constantly changing code. It's crucial to understand this vulnerability to safeguard your vehicle.

Solution Overview: The primary objective of our project is to construct a functional prototype capable of recording rolling codes and performing the rollback task. This will provide us with valuable insights into the crucial fob learning process, a fundamental aspect of automotive security and the rollback attack.

Technical Details: We will leverage FS1000A, Digispark, and SDR environment to evaluate each strategy of the RollBack attack. This setup will allow us to thoroughly evaluate each strategy involved in the RollBack attack. We will also attempt to reverse-engineer key fobs to understand the root cause better.

Data & Resources: Access to signals sent from vehicle key fobs will be required.. To facilitate this, we are actively working on obtaining the necessary permissions and tools to capture these signals. Based on insights from the referenced paper, we have already identified specific vehicle models vulnerable to the RollBack attack.

Milestones: Our project roadmap is outlined through a series of pivotal milestones:

1. Analyze RollBack Attack: Conduct an in-depth analysis to understand the RollBack attack, understanding their distinct strategies and implications.
2. Implement the Rollback System: Develop and implement a functional prototype of the rollback system. That system should be capable of executing the RollBack attack and demonstrating its potential security risks.
3. Analyze Real Key Fobs: Engage in reverse-engineering real key fobs to analyze their functioning and vulnerabilities We will aim to grasp the underlying mechanisms to prevent the RollBack attack.
4. Evaluate Vulnerable Vehicles using our Rollback System: Thoroughly test our rollback system on allowed vehicle models and assessing its ability to compromise key fob security and access mechanisms.

Benefits:

Primary Benefits: The study will offer CPS researchers essential countermeasures combating the RollBack attack, thereby enhancing overall vehicle security.

Secondary Benefits: Insights gained will uncover the root causes and aid in enhancing the design of rolling code systems. Thereby, informing the manufacturers of better countermeasure strategies for vehicle manufacturers.

Potential Challenges and Risks:

- Access Limitations: Limited access to vulnerable vehicles and key fobs may constrain testing.
- Root Cause Identification: Identifying the root cause is easier with documentation and schematics. We will collaborate with manufacturers.
- Responsible Disclosure: Responsible disclosure principles will guide our real-world testing and mitigation analysis.

List of Equipment required:

1. FS1000A Transmitter 433 MHz - (1 set):	$8
2. FS1000A Transmitter 315 MHz - (1 set):	$5
3. Digispark Module (ATTINY85) -	$8
4. SDR that has a range of 25MHz-1760MHz:	$15
Approximate Expense / Budget:	$36

References:

[1] RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems.