[1]

Enhancing Automotive Cybersecurity

Jillian Moorcroft, Jon Marien, Aaron Briand, Hala Alwash

991625656, 991476393, 991644564, 991471580

INFO49402: ISS Graduation Project (Phase 2)

Professors: Ali Hassan, George Mikhailov

Table of Contents

Enhancing Automotive Cybersecurity

1500–2500 words

***Abstract* - As car theft methods become smarter, vehicle security needs to keep up. Our capstone project, *Enhancing Automotive Cybersecurity*, explores this challenge by creating a proof-of-concept intrusion detection system that plugs right into a car's USB port. The idea is simple: detect suspicious radio frequency (RF) signals—for example those used in relay attacks—and alert the driver before it's too late. We built a working prototype that monitors incoming RF signals, flags anything unusual, and generates an alert through a connected app. Along the way, we tackled technical challenges and coordinated across roles. This project not only gave us hands-on experience blending hardware and software but also showed how even a small device can help make vehicles at least safer. This project highlights the importance of cybersecurity in automotive innovation and provides a foundation for future development and deployment of in-vehicle threat detection systems.**

Index Terms - Intrusion Detection System, USB, Wi-Fi, Bluetooth, Radio Frequency, Automotive Cybersecurity

Introduction

Our project, titled *Enhancing Automotive Cybersecurity*, presents a physical proof of concept designed to detect incoming signals to a vehicle and categorize them as benign, suspicious, or malicious. All detected signals are logged, while suspicious and malicious signals trigger alerts based on predefined categorizations. This capstone contributes to the field of automotive cybersecurity by exploring how lightweight, accessible Intrusion Detection System (IDS) technology can help bridge the gap between advanced threats and everyday vehicle security—especially for consumers who may not have access to high-end protection systems.

Although our solution does not address all forms of car theft—particularly those involving physical break-ins such as window smashing and hot-wiring—it provides a strong foundation for scalability and future enhancements in vehicle cybersecurity.

Problem Statement

In recent years, vehicle theft has evolved rapidly, especially in Canada. Criminals can now use low-cost radio frequency (RF) tools to exploit vulnerabilities in modern cars. This method called relay attacks which involves intercepting the signal from a key fob and amplifying it to trick the car into thinking the key is nearby, allowing unauthorized access or even starting of the vehicle. Intercepting and amplification of key fob signals to unlock and start vehicles without physical access, are becoming alarmingly common. In Canada alone, car theft insurance claims reached over $1.5 billion in 2023, a 254% increase since 2018. Despite this growing threat, most vehicles today still lack real-time intrusion monitoring. Many existing security measures are reactive, activating only after a breach occurs. There's also a significant gap in consumer awareness and education around these modern attack methods. In response to these challenges, our capstone project proposes a practical and accessible solution aimed at detecting anomalies signals in real time and enhancing overall vehicle security.

Our Solution

Our project tackles a growing problem that affects everyday drivers—car theft through wireless attacks. By creating a device that can detect and alert users to suspicious RF activity in real time, we're aiming to give people more control over their vehicle's security, without needing expensive or complicated systems.

The prototype we developed shows that even a small, affordable add-on—like a USB-powered dongle that cost $200—can make a difference when it comes to early detection of potential threats. It empowers users with information and awareness, which is often missing in current

vehicle security systems. Beyond the technical side, this project had a big impact on us as a team. It pushed us to think creatively, manage timelines, and apply our classroom knowledge to a real-world problem with real consequences.

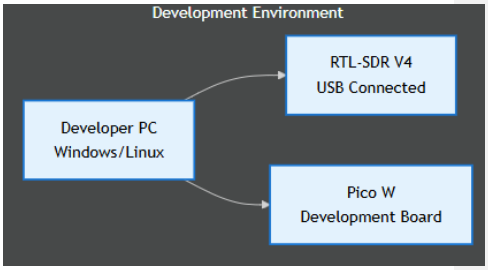
Building on this idea, our solution is designed using lightweight and affordable components that work together to monitor and analyze RF signals around the vehicle. At the core of the system is a USB-powered Software Defined Radio (SDR) plugged into a Raspberry Pi. This setup runs custom Python scripts that listen for nearby signals and evaluate them in real time. Based on defined patterns and thresholds, the system classifies these signals as benign, suspicious, or malicious—allowing users to stay informed and act when needed.

A) Hardware and Function

HARDWARE	PROGRAMMING	FUNCTION
RLT2832U: Software Defined Radio [SDR]	SDR comes pre-programmed	Used to receive incoming signals
PN532: NFC Module	MicroPython	Physical Notifications
Breadboard + Jumper Cables	N/A	Connecting the SDR to the PN532
Raspberry Pi Pico 2W	MicroPython	Alert Controller: Wi-Fi
N/A	Python + Pydantic	Event Classification
N/A	Python + NumPy	Signal Processing
N/A	Python + asyncio	TCP Event Distribution
N/A	Python + Rich	CLI Dashboard

B) Configuration

Since this is a proof-of-concept design, the hardware configuration isn't all contained in a case. Some of the components are connected through a host computer instead of directly. The hardware is configured so that the PN532 is connected to the Pico 2W through the Breadboard and jumper cables. The Pico 2W has a USB dongle connection, it is plugged into the host computer. In another USB port on the host computer, the SDR is plugged in.



C) Code

Important Code Snippets

D) Deployment

How to set up the environment

How to run the code in the command line

Commented [GU1]: For Jon to add

Results

During our testing phase, the prototype successfully detected various RF signals and was able to flag abnormal activity based on our predefined thresholds. The system categorized signals as benign, suspicious, or malicious in real-time and generated alerts accordingly. The results demonstrated the feasibility of our lightweight intrusion detection concept in identifying potential wireless threats around the vehicle. Below is a snapshot of our live detection output as captured during testing. **(JILL UPLOAD THE SCREENSHOT AND DESCRIPTION)**

Commented [GU2]: screenshot and description

Limitation

While our prototype shows promising results, there are several limitations to consider. First, the device is only designed to detect anomalous radio frequency (RF) signals. It doesn't cover threats that come through wired connections, such as the **OBD-II port** (a standardized diagnostic port used by mechanics to access vehicle data) or the **CAN bus system** (the internal network that allows a car's various

electronic components to communicate with each other), especially when these do not emit any RF signals. Additionally, since the device runs on USB power, it requires a vehicle with a consistently powered USB port. This may not be compatible with older cars that lack USB ports or newer ones that only have USB-C, as our current setup uses USB-A. Another challenge lies in signal filtering—while we implemented a context-aware threshold of -60dBm to reduce false positives, accurately distinguishing between legitimate and suspicious signals remains tricky and may still lead to occasional errors. Environmental conditions like extreme heat or cold could also affect the long-term performance of the hardware. On top of that, the device has not yet gone through any official certification processes, which would be necessary for real-world deployment. Lastly, it's important to note that our system focuses on detection and alerts—it doesn't actively stop attacks. That means drivers would still need to take action themselves once alerted to a potential threat.

Protentional Future Work

Looking ahead, there are several exciting directions this project could take. One major step would be moving from simple detection to actual prevention, which means going a step further — not just detecting a possible threat, but taking action to stop it, that would be by building in countermeasures that could temporarily disable certain communication channels or trigger an in-car alarm when a threat is detected. The user experience could also be made more intuitive, allowing drivers to customize alert profiles and signal thresholds to better suit their personal needs and driving environments. Power is another area where we see room for improvement. In the future, the device could be designed to power itself using energy-harvesting methods—like small solar panels or vibrations from the car while it's moving. This would reduce the need to rely on the car's USB port and make the system more flexible and compatible with different types of vehicles.

On the intelligence side, integrating machine learning would allow the device to adapt to a vehicle's normal RF behavior over time, improving accuracy and reducing false alarms. Finally, this solution could also be expanded for larger-scale use cases, such as fleet management—where operators could track and monitor the security status of multiple vehicles from one central system. To make that kind of deployment possible, securing the right regulatory certifications will be a key next step. There's still a lot of potential to unlock, and with each improvement, we move closer to making everyday vehicle security smarter, stronger, and more accessible.

Commented [GU3]: I dont know about this part

Commented [GU4R3]: is it good here?

Conclusion

This project started with a simple question: what if everyday drivers had a way to spot car theft attempts *before* it was too late? In a time when vehicles are being stolen using wireless relay attacks—without broken glass or loud alarms—we saw a clear gap in how cars are protected, especially for people who don't have access to expensive, high-end systems. So, we built something. A small, USB-powered device that listens for suspicious radio signals in real time and gives drivers an early warning when something isn't right. It may not stop a thief in their tracks, but it puts the power back in the driver's hands—because knowing there's a threat is the first step to stopping it. This wasn't just a technical exercise. It pushed us as a team to navigate real-world challenges, trial-and-error testing, and limitations in hardware and signal filtering. But those obstacles became part of the learning. We figured out how to turn a big problem into a functional, scalable solution—and we did it on a tight budget, with a simple goal: make cars harder to steal. Most of all, this project showed us that cybersecurity isn't just for computers. It's about protecting the things people depend on every day. And while this prototype is just the beginning, we're leaving

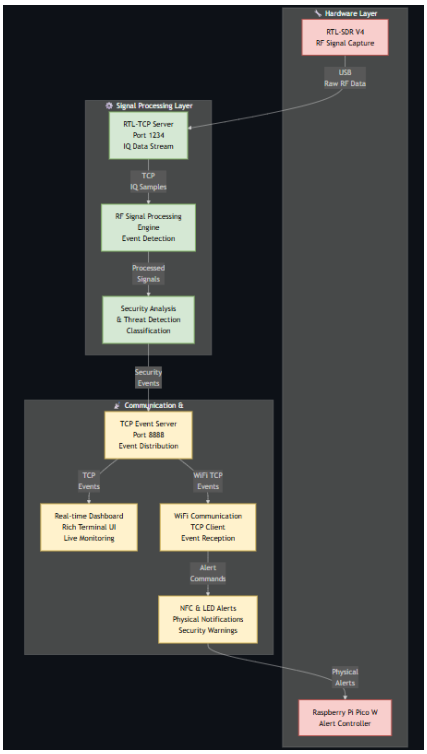
it with a working solution, a clear vision for the future, and the confidence that small ideas—when built with purpose—can make a real impact.

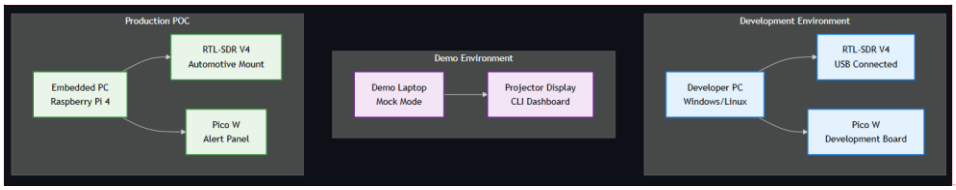
References

[1] "Automotive Cybersecurity Market size worth US$11.874 billion by 2029". Knowledge Sourcing Intelligence. https://knowledge-sourcing.com/resources/press-releases/automotive-cybersecurity-market/ (accessed 26 Jan 2025)

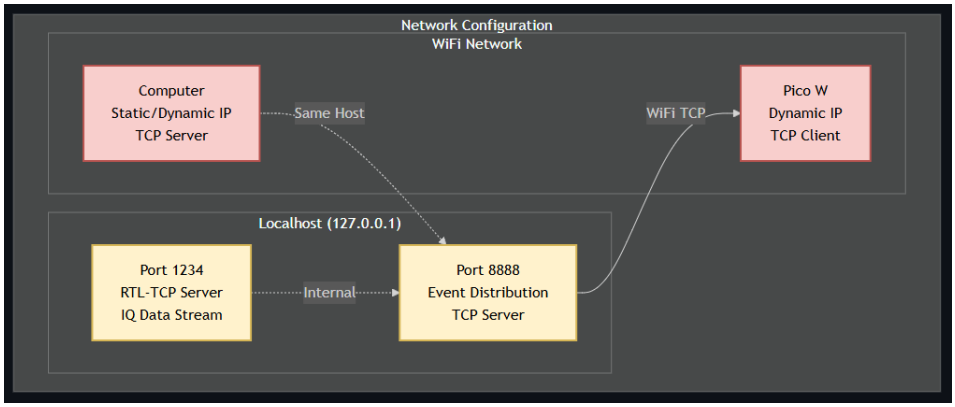
Appendix

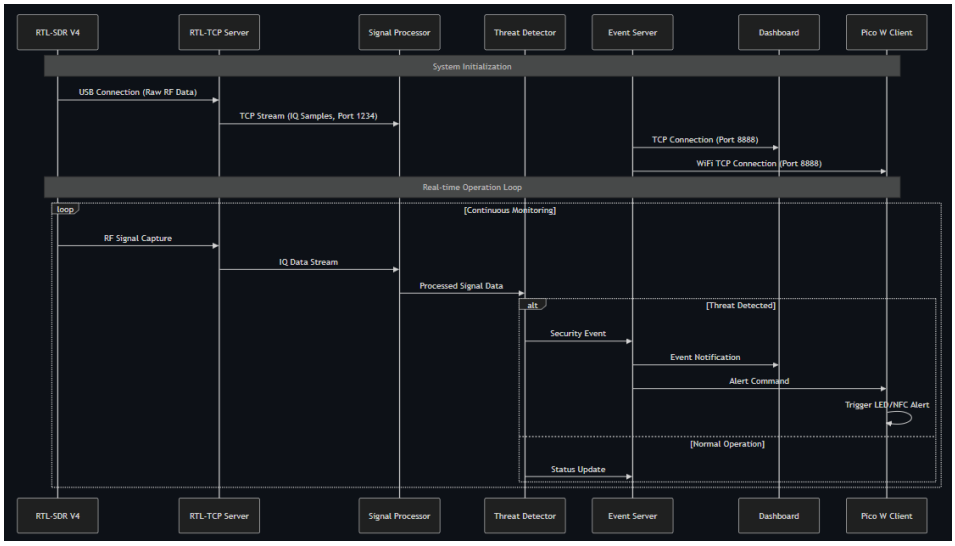
Commented [GU5]: do we need this here?

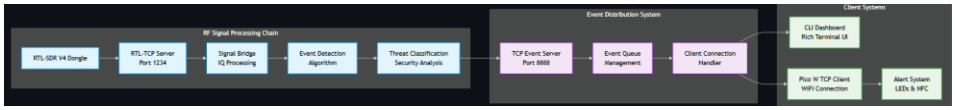




Commented [GU6]: do we need this here?


Network Configuration
WiFi Network
Computer
Static/Dynamic IP
TCP Server
Same Host
WiFi TCP
Pico W
Dynamic IP
TCP Client
Localhost (127.0.0.1)
Port 1234
RTL-TCP Server
IQ Data Stream
Internal
Port 8888
Event Distribution
TCP Server


RTL-SDR V4
RTL-TCP Server
Signal Processor
Threat Detector
Event Server
Dashboard
Pico W Client
System Initialization
USB Connection (Raw RF Data)
TCP Stream (IQ Samples, Port 1234)
TCP Connection (Port 8888)
WiFi TCP Connection (Port 8888)
Real-time Operation Loop
loop
[Continuous Monitoring]
RF Signal Capture
IQ Data Stream
Processed Signal Data
alt
[Threat Detected]
Security Event
Event Notification
Alert Command
Trigger LED/NFC Alert
[Normal Operation]
Status Update


RF Signal Processing Chain
RTL-SDR V4 Dongle
RTL-TCP Server Port 1234
Signal Bridge IQ Processing
Event Detection Algorithm
Threat Classification Security Analysis
Event Distribution System
TCP Event Server Port 8888
Event Queue Management
Client Connection Handler
Client Systems
CLI Dashboard Rich Terminal UI
Pico W TCP Client WiFi Connection
Alert System LEDs & NFC