

FLORIDA INTERNATIONAL UNIVERSITY



Hacking AI Race Strategist

Professor: Masoud Sadjadi

Product Owner: Ashley Francis

Team: Ashley Francis, Reinaldo Contreras, Jamahl Davis, Erik Pereda, Santiago Vargas

AI Race Strategist v.s. Spoofing

AI Race Strategist

- Race engineers are tasked with making swift decisions to maximize the efficiency of driving strategies.
- AI tool of this model uses machine learning to analyze historical and real-time data.
- Can adjust strategy based on weather, track conditions, and any other added variables.
- Does not replace the role of a race strategy engineer.

Spoofing

- Interception or injection of data, this can include fake values, sensor readings, or communication attacks.
- Spoofed telemetry in motorsports can result in corrupted tire or lap data that is critical for producing strategy patterns in the algorithm.
- Our project simulates this by injecting manipulated data to test system security, showcasing the danger of this attack.

Significance of Securing Systems Early On

- Showcases how artificial intelligence can enhance race strategy through data-driven decisions
- Highlights the importance of protecting telemetry data from spoofing or manipulation to prevent seriously dangerous scenarios
- Emphasizes the real-world need for encrypted AI systems in the motorsports field (connected vehicles too!)
- Baselines a foundational prototype that combines prediction + automation + cybersecurity
- Educates users, engineers, and experts alike on how attacks can impede high achieving results

Real-Life Examples

- Spoofing Attack Scenario in Formula 1

Drivers competing at high speeds may undergo spoofing attacks where values are heavily under/overestimated, causing race strategy engineers to suggest dangerous changes.

- Tesla Model X Key Fob 2017

Researchers discovered the set up protocol for the Tesla Model X key fob to be easily bypassed, resulting in unauthorized connections and remote connections.

- Chevrolet Corvette OBD-II Port 2015

OBD-II ports in Corvettes were found to be an open port for anyone to send remote commands to vehicles which could have included functions that messed with the wipers, radio, lights, and brakes.

Project Workflow

Workflow Application

Car → Telemetry Telemetry → AI Race Strategist

Project Set Up

Data Collection → Cleansing → Algorithm Development (Strategy) → Simulated

Attacks (Bluetooth Hijacking & Spoofing) → Mitigation Techniques → Incident Report

Security Integration

- Encrypted Connections
 - Securing these connections from the start greatly minimizes the risk for open attacks to happen, including any other basic level wireless attack.
- Anomaly Detection
 - An algorithm to detect abnormalities within the inputted data to easily identify injections or interferences.
- Traffic logging
 - Log all traffic that enters and exits to keep tabs. Great for auditing.

Threat & Risk Identification

Threats

- Bluetooth Spoofing/Hijacking
(known attack)
- Data Poisoning
- Denial of Service Attacks
- Unauthorized Access

Risks

- Incorrect Algorithm/Strategy
- Unsafe Driver/Engineer
- System Outages
- Delayed Patch Deployment
- Hidden Advantages

Risk Matrix

Likelihood

Impact

	LOW	MEDIUM	HIGH
HIGH	Unsafe Driver/ Engineer Decisions	Bluetooth Spoofing / Hijacking	Bluetooth Spoofing / Hijacking
MEDIUM	Unsafe Driver / Engineer Decisions	Data Poisoning	Denial of Service Attack
		System Outages	Incorrect Algorithm / Strategy
LOW	Unsafe Advantages	Delayed Patch Deployment	Delayed Patch Deployment

Mitigation Techniques

- Zero Trust Principle & CIA Triad

Authorized individuals should have a timed limit on how long they can access systems. Maintaining confidentiality of what occurs and keeping the integrity is vital, all while supplying consistent availability.

- Bluetooth Pairing Protocols

Bluetooth pairing should only remain open for 2 minutes to establish new connections and should undergo pin confirmation on both ends to ensure accuracy.

- MAC Address Detection

Implemented through anomaly detection, would be able to detect unauthorized MAC addresses.

Incident Response Plan

- Timeline: Begins from the moment the algorithm starts operations up until the system has been isolated.
- Detection: Anomaly Detection picks up on abnormal telemetry data, indicated as manually inputted values.
- Investigation: Tracks where the packets were sent, received, and intercepted to potentially identify the source and the attack vector.
- Recovery: System immediately terminates session to avoid further infiltration and a backup or physical drive is provided to collect data but strategy will not be in use.
- Prevention: Trace steps, include patches and update address detection rules along with reviewing any open ports.

5 & 10-Year Prospect with Integrated AI in Vehicles

5-year outlook (2030)

- AI systems become standard across collegiate racing, moving into high-tier series.
- Increased dependence on wireless telemetry, increasing attack vectors.
- Predictive models detect early signs of vehicle failure with greater accuracy.

10-year outlook (2035)

- Total integration across all racing series, making its way to average vehicles.
- Human engineers become supervisors to these models.
- Motorsports organizations adopt AI regulations and data governance policies.

Future Proofing Mitigation Strategies

- Direct Security Layer in Models
- Creation of Digital Twin (Simulated v.s. Real-Time)
- Switch Methods for Wireless Compromise
- Dedicated Team of Cybersecurity Experts
- Hardware with TPM Chips

Conclusion

- Our project demonstrates the how artificial intelligence race strategy can optimize decisions using telemetry data, while remaining vulnerable to spoofing/wireless attacks.
- Anomaly detection and security integration within the algorithm can prevent data manipulations and exposure.
- Real-world examples emphasize the dire need for vehicle cybersecurity.
- Future prospects include standardized integrations of AI, anti-attack methods, failsafes, and greater emphasis on the social awareness of security practices.

Reference

- Abrar, M. M., Yousseef, A., Islam, R., Satam, S., Latibari, B. S., Hariri, S., Shao, S., Salehi, S., & Satam, P. (2024). GPS-IDS: An anomaly-based GPS spoofing attack detection framework for autonomous vehicles [Preprint]. arXiv. <https://arxiv.org/abs/2405.08359v2>
- Dommari, S. (2025). Cybersecurity in autonomous vehicles: Safeguarding connected transportation systems. ASRJETS, 102(1), 76–108.
https://asrjetsjournal.org/index.php/American_Scientific_Journal/article/view/11640/2840
- Morad, I., & Yako, Y. (2025). A systematic literature review on cybersecurity in autonomous vehicles. Jönköping University, School of Engineering, Computer Science and Informatics.
<https://hj.diva-portal.org/smash/get/diva2%3A1976123/FULLTEXT01.pdf>
- Rilian Technologies. (2025, January 15). The evolution of AI-driven cyberthreats in Formula 1 and the automotive industry. Rilian Technologies Blog.
<https://www.riliantech.com/blogs/the-evolution-of-ai-driven-cyberthreats-in-formula-1-and-the-automotive-industry>