



IDAHO SCIENTIFIC'S SECURE HELIOS DEMONSTRATION



Team: Macallyster Edmondson, Robert Walko, Kyle LeDoux, Chadwick Goodall, Jackie Lee
Mentors: Dr. Yacine Chakhchoukh, Dr. James Frenzel, Phillip Hagen
Sponsor Reps: Rick Hoover, Andrew Weiler

Objective:

Demonstrate the security capabilities of Idaho Scientific's hardware secure, Helios Processor in the form of a live demonstration.

Value Proposition:

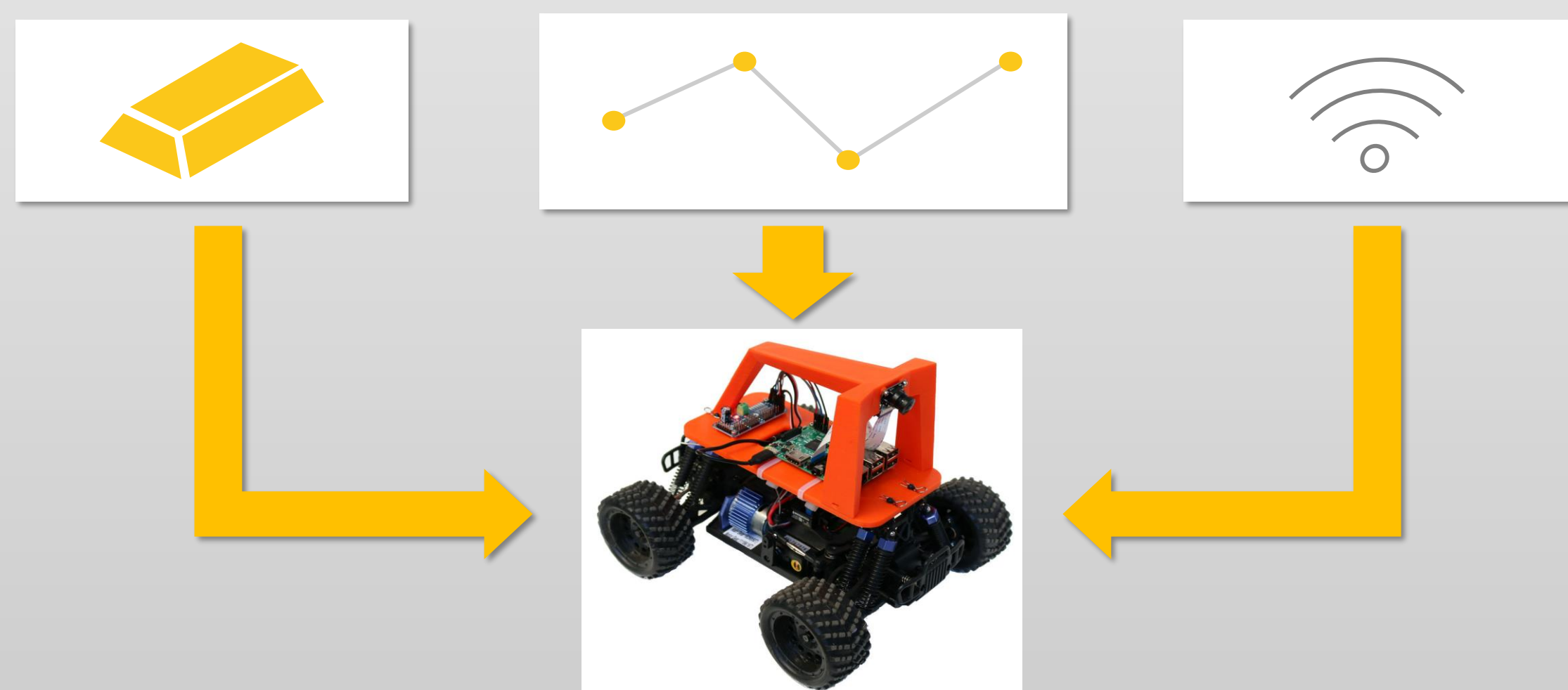
Large Scale Problem: Contemporary infrastructure hardware can be reverse engineered by threat actors.

Sponsor's Solution: Solve problem at hardware level by creating a secure processor (Helios) that cannot be reverse engineered.

Our Contribution: Demonstrate how Helios protects against multiple types of software vulnerabilities.

Background & Key Requirements:

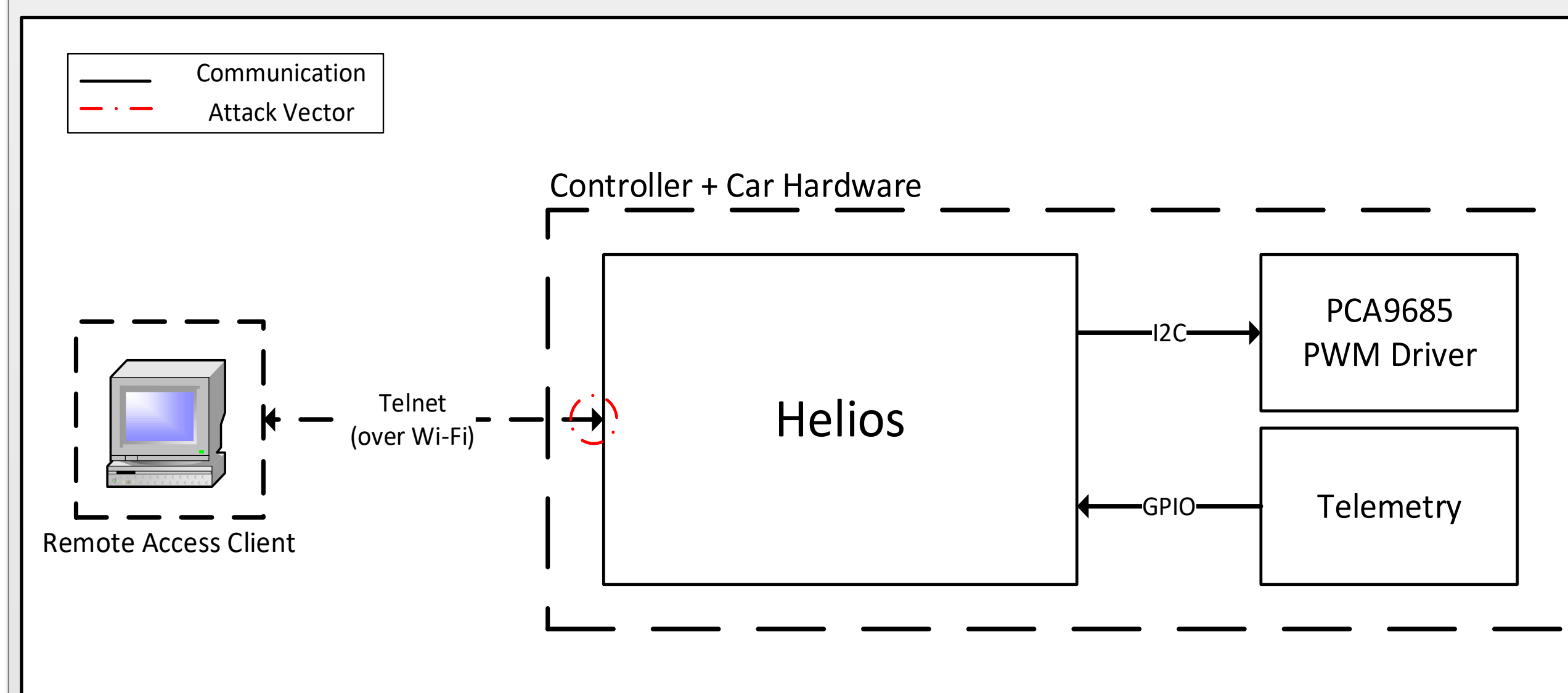
Helios should control an RC car autonomously with software designed by the team & must be able to communicate wirelessly with the vehicle. To demonstrate the security features of Helios, three separate cyberattacks should be conducted, including a memory corruption attack, a reverse engineering attack & a binary patching attack.



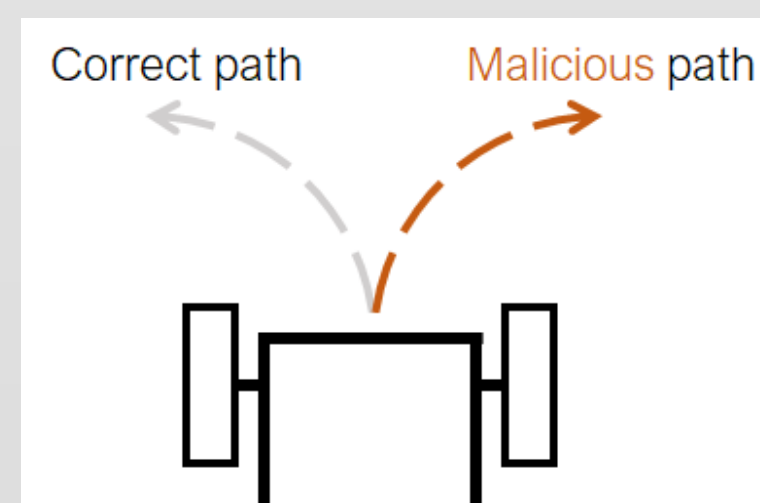
Acknowledgements:

Our team extends many thanks to our very helpful mentors & sponsor representatives. This project served as a great learning opportunity for our team, & we hope ISCI can make use of our work.

Conceptual Development:

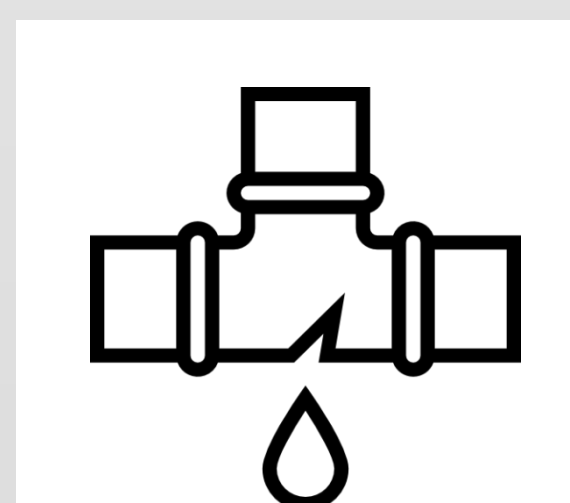


Memory Corruption



We'll write malicious code into raw memory which will cause the car to behave erroneously

Reverse Engineering

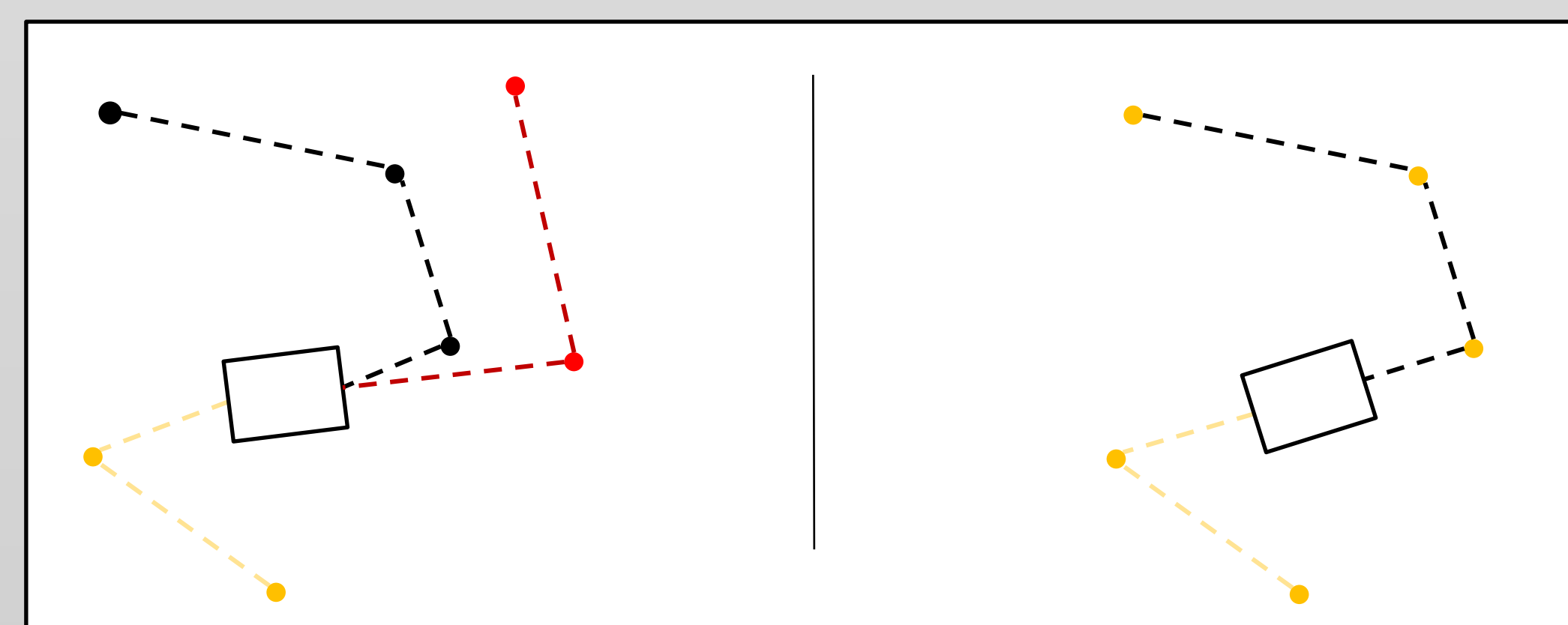


The program will leak confidential information

Binary Patching

000101010
 100010101
 011101010
 100101001

The car's navigation software will be permanently modified

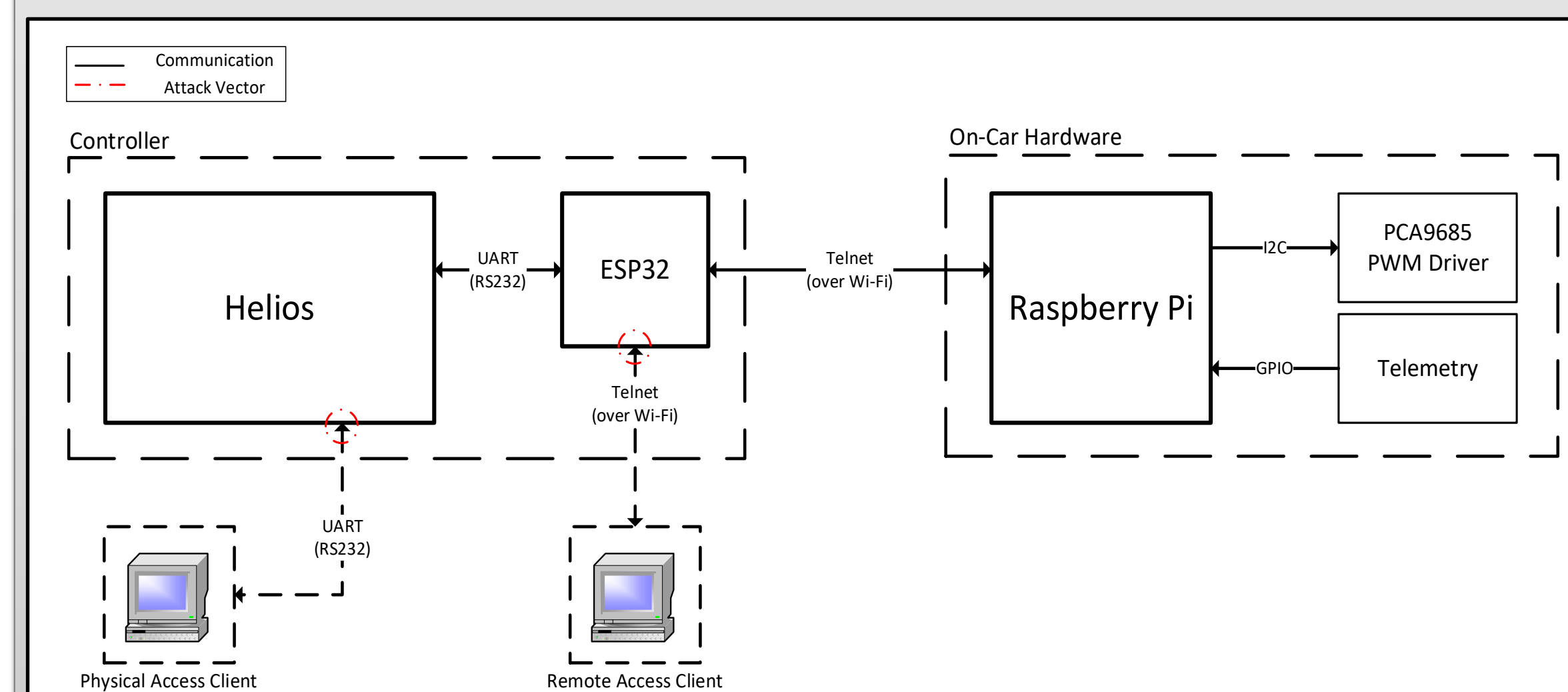


Helios (Insecure)

Helios (Secure)

Final Design:

Engineering time in this project was primarily focused on the system design: communication protocol; format, & reliability; gathering & normalization of telemetry data; physical connections of hardware. Software attacks were developed & carried out in a prototyping environment, on Helios.



Validation:

Our team focused on unit & integration testing philosophy. This entails testing each software/hardware component, integrating that component into the system, & then testing the overall system.

Summary/Conclusion, Recommendations:

Our team successfully carried out three cyber-attacks on an insecure version of Helios, proving the limitations of common processors. Solving the problem at a hardware level is a necessary step in preventing such attacks on critical infrastructure, which is what ISCI aims to accomplish with secure Helios. Recommendations for further development are to increase the capability of the navigation software to utilize automated control software, & to develop more sophisticated attacks against the Helios processor.



2023 Capstone Project