Detection and Mitigation of Anomalous Behavior in Embedded Automotive Networks

sekark1@umbc.edu
240-205-1955

13204 Trumpet Place
Silver Spring, MD 20904

Sekar Kulandaivel, Jackson Schmandt, Matthew Fertig, Dr. Nilanjan Banerjee
Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County, Baltimore, MD 21250

ABSTRACT

Safety and security for drivers becomes crucial to the future of the automotive industry as advanced electronics permeate a vehicle's control systems. Electronic and wireless components within an embedded automotive network expose vulnerabilities to malicious attacks from internal and external sources. In order to combat a malicious attack on a vehicle's network, this work focused on using physical sensors embedded in a vehicle to classify normal driver behavior versus behavior resulting from an infiltration by an external agent. To investigate this method of intrusion detection, we accessed the raw communication data between various electronic control units (ECUs) and gathered pedal depression and steering wheel angle data from textile-based capacitive sensors. Our model for typical driver behavior includes comparison of the physical sensor readings of the steering wheel, brake pedal, and accelerator pedal to the data received from the ECUs. The resulting deployable attachment for an automobile's on-board diagnostics port detects and mitigates a variety of infiltrations from external agents, which serves to protect drivers from dangerous attempts to disrupt or disable electronic systems within their vehicles.

Introduction

State of Automotive Security

Consumers demand additional functionality. Automakers and government demand safety for their customers.

- Additional functionality includes Wi-Fi hotspot, GPS, Bluetooth, Internet applications, remote keyless entry, etc.
- Customer safety includes a variety of cyber-physical systems, such as Intelligent Parking Assist and Adaptive Cruise Control

Table of possible attack vectors due to safety-related cyber-physical systems

	Steering Wheel	Brake Pedal	Accelerator Pedal
Intelligent Parking Assist	X	X	X
Lane Keeping Assist	X	X	
Emergency Brake Assist		X	
Adaptive Cruise Control	X	X	X
Forward Collision Mitigation		X	

Previous Research

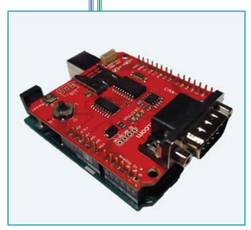
Vehicles used in previous research are 2010 Toyota Prius (left) and 2010 Ford Escape (right)

Adventures in Automotive Networks and Control Units [1]

- Similar vehicles to previous research allows replication of attacks
- **2010 Toyota Prius** → Dr. Nilanjan Banerjee's 2010 Toyota Prius
- **2010 Ford Escape** → Sekar Kulandaivel's 2008 Ford Escape

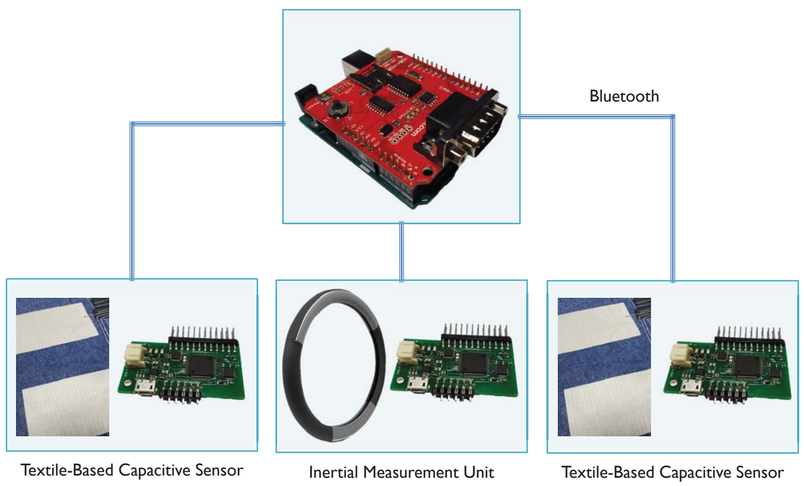
INTRUSION DETECTION SYSTEM

Steering Wheel Position and Pedal Depression ECU Network



Arduino Uno Microcontroller with CAN Bus Shield

Physical Sensors for True Position and Depression Values



Analyzing CAN Bus Traffic on Prius and Escape

Message IDs Found in Miller & Valasek Paper and in Our Vehicles

- Messages for 2010 Toyota Prius
  - CAN ID 0025 → Steering Wheel Angle
  - CAN ID 0224 → Brake Pedal Position Sensor
  - CAN ID 0230 → Brake Sensor
  - CAN ID 0245 → Accelerator Pedal Sensor
- Messages for 2008 Ford Escape
  - CAN ID 0080 → Steering Wheel Angle
  - CAN ID 0200 → Brake and Accelerator Pedal Sensor

DISCUSSION

CAN ID 0224 Byte-Field Description for 2010 Toyota Prius [1]

CAN ID	*0224*
Description	*Brake pedal position sensor*
Length	*08*
Data[0]	*State 0x00 unengaged | 0x20 engaged*
Data[1]	*00*
Data[2]	*00*
Data[3]	*00*
Data[4]	*Position Major (carry over for position minor) Max 0x3*
Data[5]	*Position Minor (00-FF carry over add or sub from Major)*
Data[6]	*00*
Data[7]	*08*
Example	*I02, IDL: 24, Len: 08, Data: 20 00 00 00 00 09 00 08*
Decode	*Brake at 0009 %*
Notes	*Brake position may be percent or other measurement*

Example of CAN ID 0224 Data

```
   TS -->  ID [L] AA BB CC DD EE FF GG HH
33953 --> 224 [8] 20 00 00 00 01 97 00 08
35937 --> 224 [8] 20 00 00 00 01 35 00 08
38212 --> 224 [8] 20 00 00 00 00 16 00 08
40564 --> 224 [8] 20 00 00 00 00 23 00 08
44410 --> 224 [8] 00 00 00 00 00 00 00 08
```

Analysis of the CAN Bus Traffic

1. Search for changes in CAN bus data that correspond to changes in steering wheel position and pedal depression
2. Compare received CAN bus data to data from physical sensors for steering wheel and pedals
3. Detect differences between virtual and physical data and indicate if an intruder accessed the automotive network
4. Mitigate attack by alerting driver of situation

STATUS

- Refining CAN data collection system to include a remote cellular component for performing remote attacks
- Developing integrated physical sensor network, which will include two capacitive array sensors for foot pedals and an IMU and capacitive touch sensor for steering wheel
- Planning system for comparing virtual CAN data to physical sensor data

CONCLUSION

- Development of this intrusion detection system may provide a solution to ensuring that safety-critical components of a vehicle remain unaffected by a malicious intruder

REFERENCES

[1] C. Miller and C. Valasek. "Adventures in automotive networks and control units." *DEF CON* 21 (2013): 260-264.

ACKNOWLEDGEMENTS

Many thanks to the UMBC Office of Undergraduate Education for funding this work through an Undergraduate Research Award and to Dr. Nilanjan Banerjee, Jackson Schmandt and Matthew Fertig for our collaboration on working on one of my favorite research projects.