Augmented and Autonomous Vehicle Security

Kevin Gilbert, Christopher Haster, Gilberto Rodriguez III, Hao Chen, Young Chou, Joshua Bryant
University of Texas at Austin

-

Abstract

Our research project is focused on highlighting security concerns in augmented and autonomous vehicles. We have developed and built a robotics testbed and simulator on which we can measure and apply real-world data. We primarily focus on the two coupled weak points in augmented automotive cybersecurity: wireless transceiver entry points into an unsecured Controller Area Network (CAN) and the encryption/authentication of this wireless network.

Main Objectives

Our main objectives were to design and implement a testbed on which we could launch security exploits and defenses while providing a retrospective of current automotive cybersecurity. We wished to highlight the inherit dangers of an unsecured CAN bus and demonstrate the necessity of high speed, short-term encryption. Our goals were to create a secured CAN-like protocol within a FPGA coupled with hardware encryption on which we could pipe wireless packets through. We would test this device with a set of wireless transceivers at high speeds in moving vehicles and within our robotics testbed. The realworld data we generated could then be used within a simulator in which we could measure safety and implement a variety of network protocols.

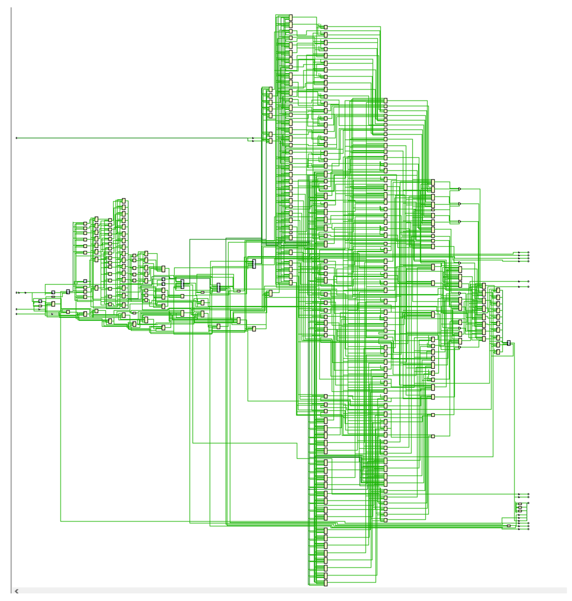
Modules

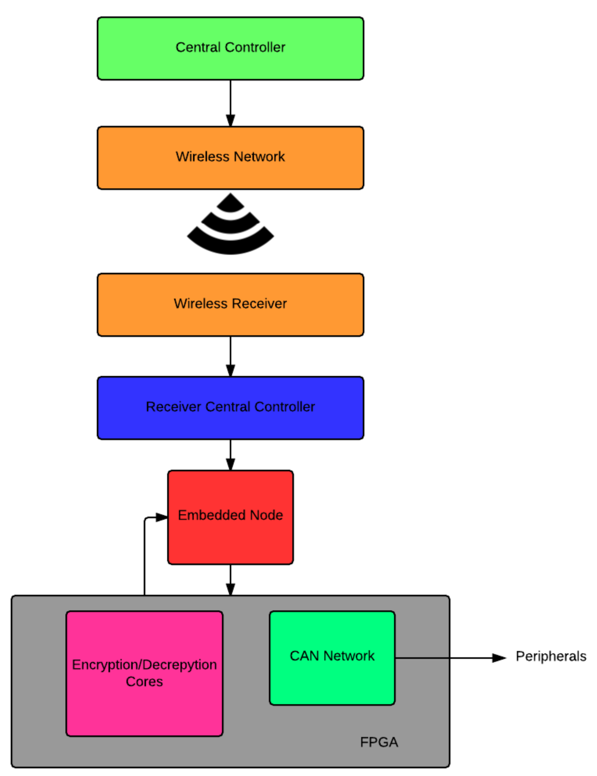
Our primary modules were broken down into:

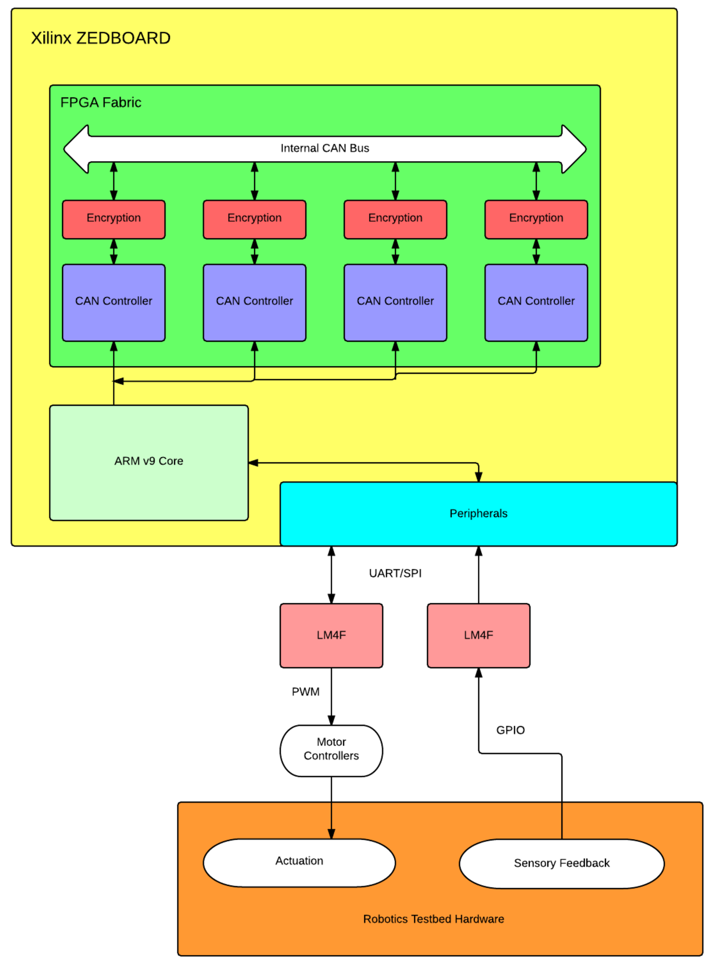
- FPGA -
  - CAN Bus
  - UART - CAN Packet Translation
  - PWM Generation
  - Hardware Encryption
- Wireless Transceivers -
  - Data Transmission
  - Software Encryption
- Robotics Testbed -
  - Data Measurement
- Embedded -
  - IMU Measurement
  - Motor Control (PID)
  - Laptop to CAN Bus Interface
  - Sensor Interface
- Simulator -
  - Network Timing Constraints

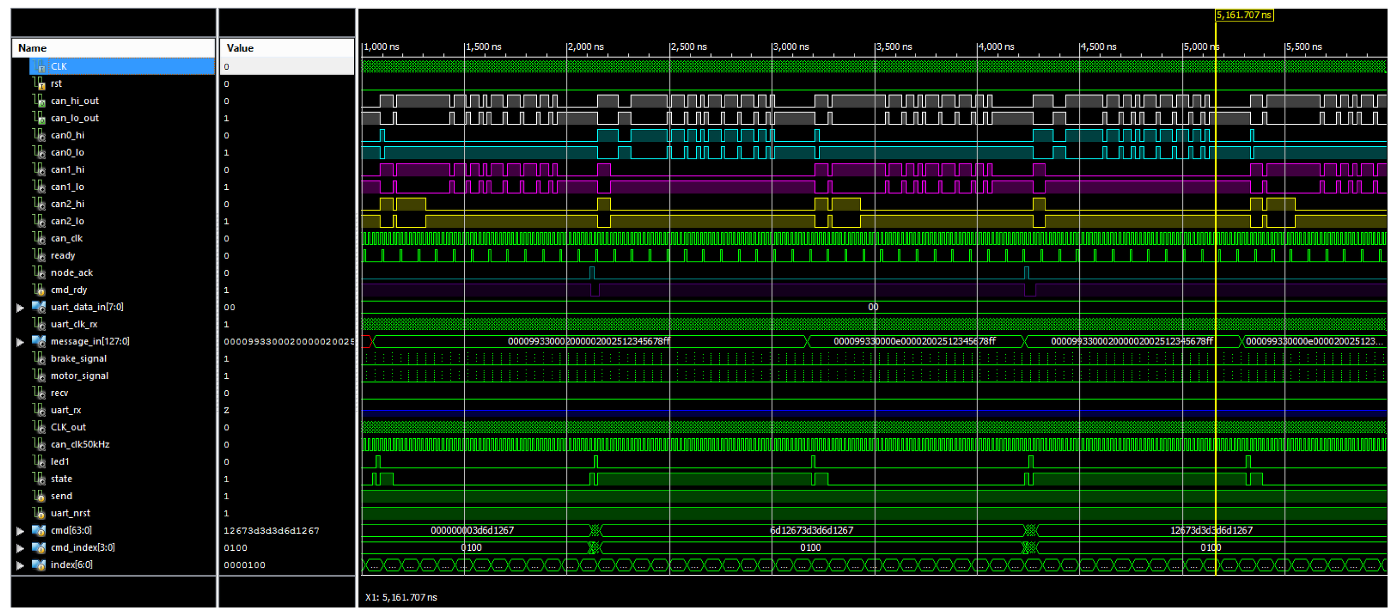
Measurements and Data

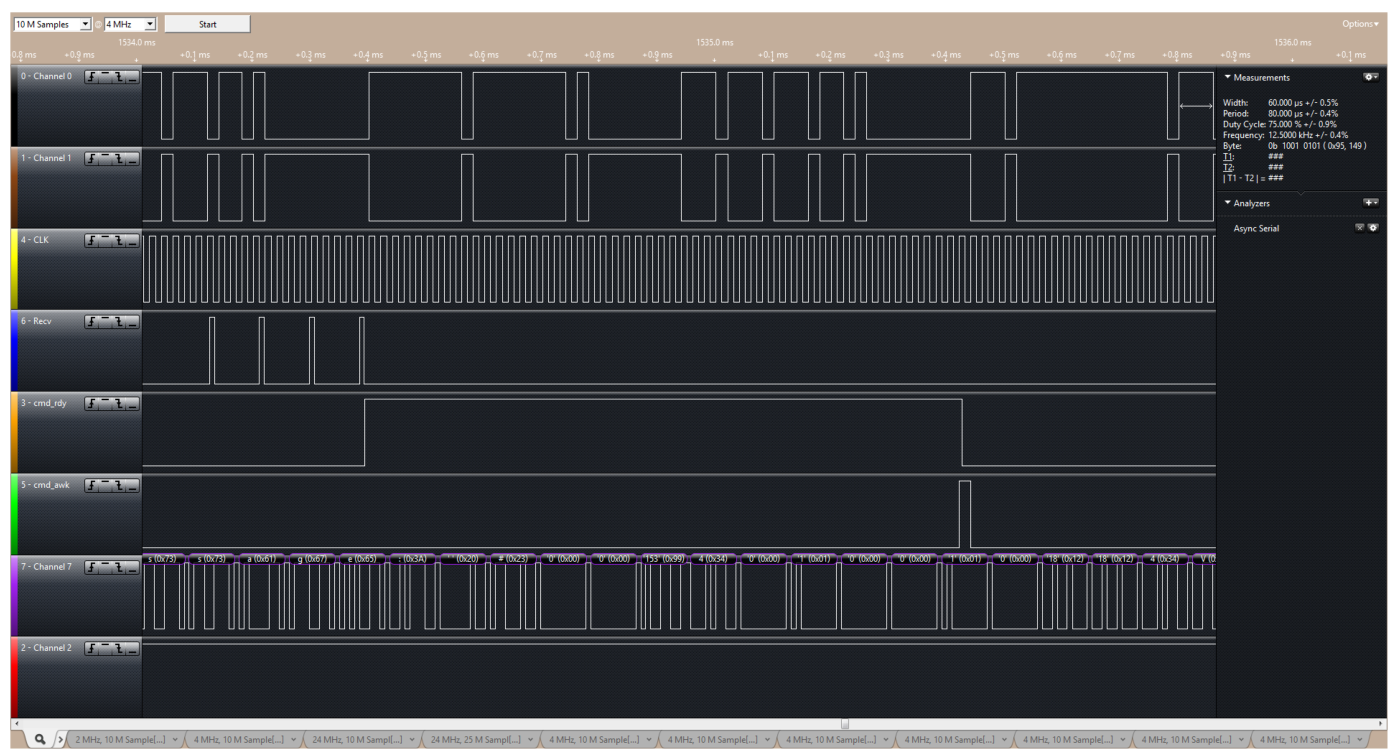
We will focus on modular specific system testing and timing constraints collected in this section. The following section will collect this data into a summary of our results.

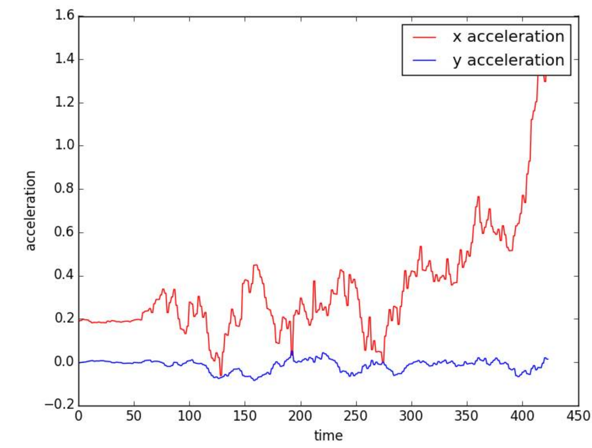


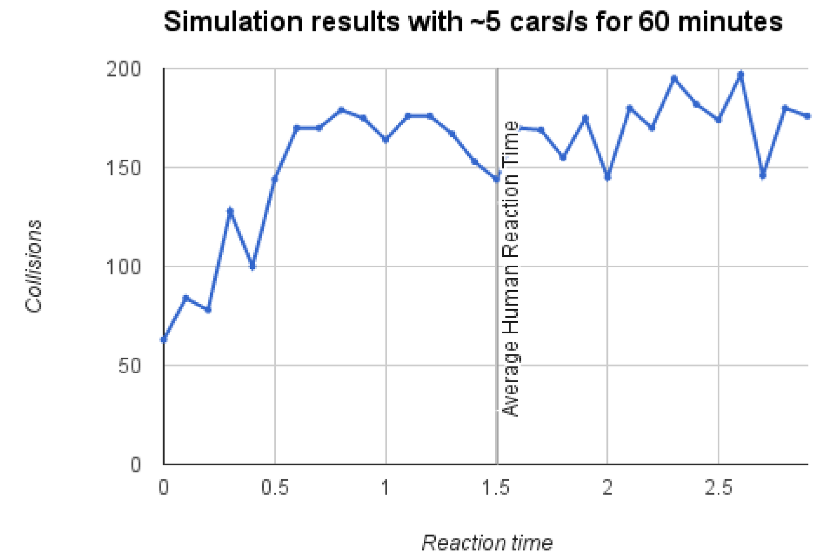


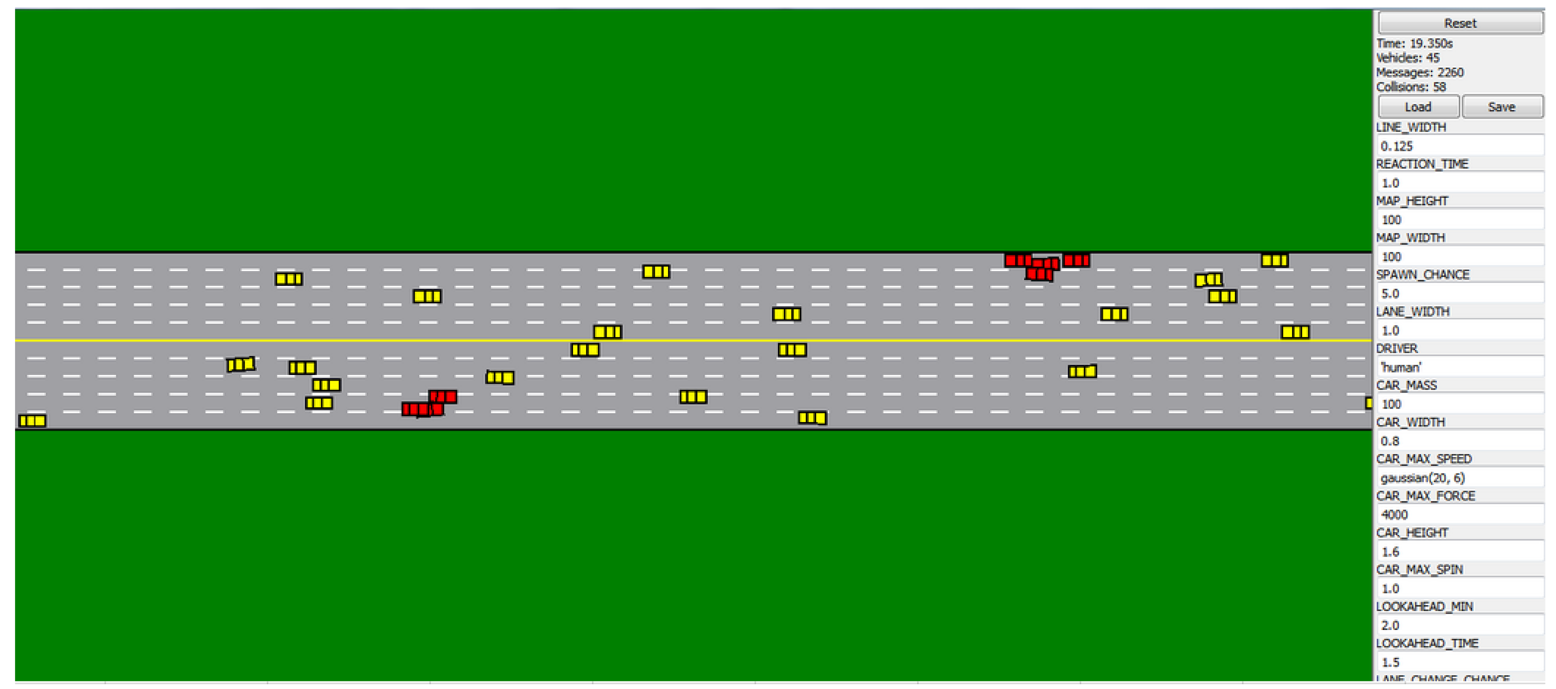












Results

Software encryption was shown to be extremely slow, taking upwards of 8.9 seconds to scramble data using a simple cipher. In addition during wireless transmission, using an ad-hoc network(typically used for long term secure channels) took several seconds on average to connect. This would not be a feasible communication method at high speeds. Utilizing high frequency channels similar to DSRC would allow for rapid bursts of data, while using hardware encryption would provide a throughput of between 20-100ns per 128-bit block (using a Tiny-AES-256 core on a Xilinx Zync FPGA running at 50MHz). The largest bottleneck in the system stemmed from the CAN bus. The simulator provides us an outlet to test communication networks in a distributed mesh network and demonstrated the benefits of increased reaction time through driver braking assistance. We implemented an abstraction layer and added a source ID field along with the concept of permission rings to our CAN bus to prevent a compromised node from gaining access to sensitive systems, utilizing the above encryption scheme in the case of a high danger node (the outwards facing wireless transceiver) needing to be able to talk directly to high security systems. However, while we were able to encrypt data at high speeds, we were unable to develop a large scale, distributed authentication scheme that could operate in the micro-milli second range. High speed car tests have been stalled due to antenna issues at the time of this poster.

Conclusions

The topic of security in interconnected vehicles is a rapidly growing and vitally important field. This project barely scratched the surface, looking primarily at the feasibility of incorporating advanced level security concepts into a high speed cyber-physical system. Our work here has set up the ground work for deeper exploration into the complex problems of authentication across millions of users in the realm of microseconds, hardened bus protocols, and the benefits connected vehicles provide in terms of driver safety.

Acknowledgements

Dr. Tiwari, TI, UT Austin