6.857 Project Proposal
Matthew Chang
Skanda Koppula
Nicolas Bravo March 20, 2015

Authentication and Encryption at the Link-Layer in Electric Vehicles

The CAN protocol is a message-based vehicle bus protocol to at the link-layer used in electric vehicles to manage battery charging, discharging, reading car diagnostics, and programming the motor controller.

Every electric vehicle in the US is required to have an OBD2 port that communicates using CAN. For internal messaging within the car's control systems, a lot of EVs on the market also use CAN (others use propietary messaging protocols (e.g. Tesla uses in-house protocols over ethernet)) [1, 2].

Unfortunately, searching through literature provides no known implementation of an authentication and encryption system to secure CAN or similar automative protocols from attacks. Though most the most critical EE components in an electric vehicle are often embedded deep in the car, it is theoretically possible to inject hardware to snoop messages and forges messages for malicious purposes. Furthermore, the mandated OBD2 port also opens potential vulnerabilities.

The 2014 BlackHat conventions started a sessions, for example, on how to play around with controlling car IO (e.g. windshield wipers, diagnostics information) given access to an OBD2, or in newer vehicles, external ethernet ports [3, 4]

Our team believes it would be interesting to (1) design and implement a layer of EAX to CAN and (2) also see how this message authentication/encryption system affects message-passing timing, especially since latency is critical in EV microcontrollers.

We were interested in using software simulators to model CAN nodes and inter-node messaging, for faster debugging/development (even though our team has access to real CAN controllers and programmers, hardware development might be slower). Our most promising find so far, an open source simulation tool: `http://rbei-etas.github.io/busmaster/`.

[1] Introduction to CAN in EVs. `http://www.ti.com/lit/an/sloa101a/sloa101a.pdf`

[2] More on OBD2 `http://hackaday.com/2013/10/29/can-hacking-protocols/`

[3] Blackhat and CAN! `http://www.canbushack.com/blog/index.php?title=automotive-electrical-systems&more=1&c=1&tb=1&pb=1`

[4] Long but interesting read. `http://illmatics.com/car_hacking.pdf`