Hardware Based Secure CAN Bus Communication

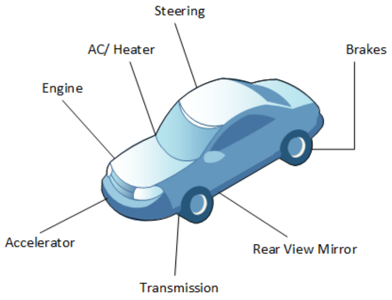
Ali Shuja Siddiqui, Jim Plusquellic *, Fareena Saqib
Dept. of Electrical and Computer Engineering, Florida Institute of Technology, Melbourne FL 32901-6892, USA
* Dept. of Electrical and Computer Engineering, University of New Mexico, Albuquerque, NM 87131-0001, USA
E-mail: asiddiqui2015@my.fit.edu, jimp@ece.unm.edu, fsaqib@fit.edu

***Abstract*—Controller Area Network (CAN) is one of the most widely used network protocol for internal communication in automobiles. Due to its open nature, it has been proven to be insecure, but since it plays an important role in the safety of a vehicle it is important that effort must be made to ensure that it is made safe from malicious entities. In our demo, we will firstly demonstrate the vulnerabilities of the bus and then a viable secure communication framework that can assure secure real time communication.**

Keywords—CAN bus, real time secure communication, Hardware security.

I. Introduction

In the recent years, the automotive industry has fallen prey to remote access attacks, where attackers have shown to gain access to entire functions of an automobile, ranging from dashboard control to critical functions such as motor acceleration, steering and the brakes[1].



These functions are handled by separate control units called Electronic Control Units (ECUs). These ECUs are connected to each other in a network. One of the most commonly used network implementation used in the automotive industry is the Controller Area Network (CAN) bus. The CAN is an inexpensive, yet reliable bus based communication protocol. This bus is susceptible to eavesdropping and malicious message injection attacks. There are some solutions that address these issues, but the common limitation in all the existing solutions is that these are either software based solutions that are not able to provide real time encryption or alternatively they are external hardware based solutions that require additional hardware and therefore extra space, cost and power.

II. Hardware Demo

In the demo, we aim to present our FPGA based real time solution for secure communication between CAN bus nodes. AES-128 encryption is used to secure the communication between two communicating nodes. To discourage the use of global master keys, we are generating per node keys using Physical Unclonable Functions (PUFs) Challenge Response Pairs (CRPs)[2]. The keys for each individual node are registered at each corresponding communicating node in a trusted environment so that no malicious node can add itself to the network. This work is based on our original publication [3].

A. *Experimental Setup*

Hardware used in our demo is as follows:

- 02 FPGAs.
- 02 CAN Transceivers.
- 01 Raspberry Pi with CAN Bus Shield.
- 01 Arduino equipped with a CAN Bus Shield.

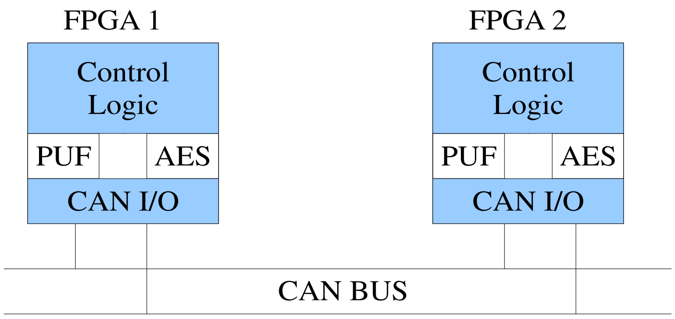


Fig. 1. Experimental setup for secure CAN Bus communication.

B. *Observables*

There are two parts in our demo. In the first part, we will demonstrate message transmission between two traditional unencrypted CAN bus nodes. Then using an Arduino with the CAN bus shield which will act as a malicious node, we will show how straightforward it is to eavesdrop the bus and will demonstrate packet injection attacks.

In the second part of the demo, the secure design of ECU and the secure framework will be demonstrated that mitigates the threats and introduces secure communication.

[1] C. Miller and C. Valasek, “Remote Exploitation of an Unaltered Passenger Vehicle,” *Black Hat USA*, 2015.

[2] W. Che, F. Saqib, and J. Plusquellic, “PUF-based authentication,” in *2015 IEEE/ACM International Conference on Computer-Aided Design (ICCAD)*, 2015, pp. 337–344.

[3] A. S. Siddiqui, Y. Gui, J. Plusquellic, and F. Saqib, “Poster: Hardware based security enhanced framework for automotives,” in *2016 IEEE Vehicular Networking Conference (VNC)*, 2016, pp. 1–2.