Assignment 2 Report

John Smith

Registration no. 03678902
E-mail: myemail@server.com

Abstract

The number of communication interfaces within modern vehicles are increasing and manufactures are replacing more and more mechanical solutions for control by electronics and software [4]. People want to access information from the internet while driving. While this could have a lot of benefits, it also has to be investigated whether these additional interfaces of a wireless car could open opportunities for hackers to attack the internal control systems of the car via the intra-vehicle communication protocols. In this report I have summarized the concept and vulnerabilities of the FlexRay protocol which is considered as successor of CAN for safety critical components.

1. Introduction

The number of communication interfaces for cars are continuously increasing. Among them are cellular connectivity, wireless internet access and remote diagnostic. Also vehicle-to-vehicle and vehicle-to-infrastructure will probably cause a large scale of cyber attacks against modern vehicles [5]. If one of the ECUs is captured by an attacker, the question is whether he can gain access to more safety-critical components of the car. This question can be answered by investigating on the security features of todays in-vehicle communication protocols. At first a short overview of the different protocols and their features is given. Table **??** summarizes the main properties of these protocols.

1.1. CAN

The Controller Area Network (CAN) is the a very common bus protocol in automotives and was developed in the 1980s. It is an event triggered protocol that sends the messages to all nodes. Each node decides according to the message ID if it wants to receive and read the message or not . The message ID is also used to indicate the priority to ensure the important messages are always transmitted first. CAN is quite robust against electromagnetic noise by using its differential wiring combined with mechanisms to detect transmission errors. Additional it features fault localization and the ability to disconnect a fault controller [7].

1.2. LIN

The Local Interconnect Network (LIN) is a newer protocol, published in 2002 as version 1.3 and intended for a lower cost, single wire implementation. It is based on the on the Enhanced ISO9141 standard. There is one master and up to 16 slaves with dynamic address assignment. The data is transmitted serial with a data rate up to $20\,\mathrm{kbp/s}$. It also offers time synchronization for nodes that do not have a stable time basis [1].

2. Conclusion

Since FelxRay was designed for reliability and not especially for security it does not address most of the security properties. Therefore any device on the bus can listen to all messages that are sent between other devices and analyze the content. It was shown by several research groups that attacks exploiting FlexRay protocol are realistic and could be used to create unintended behavior of the vehicle. With mechanisms already applied to many internet services the security of the FlexRay bus could be increased. These mechanisms include encryption, authentication signatures or special detection units that observe the bus traffic.

References

[1] http://www.edn.com/design/test-and-measurement/4391269/Debugging-automotive-serial-buses--CAN--LIN-and-FlexRay-exposed, Accessed on 15/10/2015 (cited on p. 2)

[2] Dennis K. Nilsson, Ulf E. Larson, Francesco Picasso, and Erland Jonsson – *A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay*, Springer-Verlag Berlin Heidelberg, 2009 (cited on p.)

[3] Nilsson, D.K., Larson, U.E. – *Simulated Attacks on CAN Buses: Vehicle virus.*, Proceedings of the Fifth IASTED Asian Conference on Communication Systems and Networks, 2008 (cited on p.)

[4] Sabarathinam Chockalingam and Harjinder S. Lallie – *Alarming! Security Aspects of the Wireless Vehicle: Review*, International Journal of Cyber-Security and Digital Forensics, 2014 (cited on p. 1)

[5] Gang Han, Haibo Zeng, Yaping Li, and Wenhua Dou – *SAFE: Security-Aware FlexRay Scheduling Engine*, IEEE, 2014 (cited on p. 1)

[6] *FlexRay Communications System*, Protocol Specification, Version 3.0.1 (cited on p.)

[7] Marko Wolf, André Weimerskirch, and Christof Paar – *Security in Automotive Bus Systems*, Proceedings of the Workshop on Embedded Security in Cars (escar)'04, 2004 (cited on p. 1)

[8] Fujitsu Microelectronics – *Next Generation Car Network - FlexRay*, 2006 (cited on p.)