Mobile Vehicle Cybersecurity with Onboard Key Management Iowa State University: ECpE sdmay23-15 Aayush Chanda, Alexander Freiberg, Baganesra Bhaskaran, Brian Goode, Chau Wei Lim, Michael Roling

Overview

The controllers used within a vehicle - the computers which interpret sensor data, operate a number of drive systems, and yield reliable performance - all communicate via the controller area network (CAN) bus. It is a two-line system which reduces complex wiring and allows controller communication without a host computer. The data sent on the CAN bus, therefore, will be received by each controller. It is in the interest of all parties involved - the manufacturers, operators, and third-party producers - the data is genuine. Security and safety issues arise when illegitimate controllers are placed on the vehicle's CAN bus; specifically, devices which can read and manipulate data. Similar threats can be implemented through software attacks, for example, the vehicles which communicate via cellular towers. Providing a novel solution to secure the data sent on a vehicle's CAN bus and render falsified information purposeless is the primary goal of sdmay23-15's project.

Introduction

- Project deliverables
 - Handle entire CAN frames
 - Ability to generate keys to encrypt/decrypt data
 - Functionality should be achieved without OEMs injection of confidential information;
 implications extend to 3rd parties
 - Communication operations are to meet recognized standards within the automotive industry
 - ISO and SAE
- Other project objectives
 - Encryption/decryption and Tx/Rx must be handled in an efficient manner (5mS)
 - E.g.near immediate acceleration and deceleration
 - Familiarity with other encryption/decryption methods within the automotive industry

Methodology

- Preliminary research
 - CAN functionality, J1939 Protocols, and pertinent ISO Standards
- Design proposals
 - Using of existing CRC bit field to hold encrypted data being transmitted
- Revision of design to increase scalability
- Implementation of CAN and encryption tools

Simplified Diagram of Classical CAN and CAN FD Frames:									
Classical CAN									
Identifier Field	Control Field	Data Field (0 to 8 Bytes)	CRC Field						
Nominal Bit Rate <u>CAN FD</u>									
Identifier Field	Control Field Data Field (0 to 64 Bytes) CRC Fi								
Nominal Bit Rate		Nominal or Data Bit	Rate 1						

Implementation

- Virtual simulation environment
 - Ubuntu; multiseat operation
- CAN Socket in C
 - CAN Tx/Rx
 - Multiple nodes on the CAN Bus
- CAN FD and J1939
 - Extension of CAN Frames
 - Increased bits/second
- TweetNaCl encryption
 - Efficiency
 - Box Function; nonce and MAC
 - Functionality ensures security

0009	1	158	1	00	00	00	00	00	00	00	37	7
0010	i	161	ï	00	00	05	50	01	08	00	28	P
0011	i	164	i	00	00	C0	1A	AB	00	00	13	
0007	i	166	i	DØ	32	00	36					.2.6.
0009	i	170	i	00	00	00	00	10	00	00	30	
8000	i	183	i	00	00	00		00	00	10		
0098	i	309	i	00	00	00	00	00	00	00	84	
0009	i	18E		00	00	7Å						
0010	i	191	i	01	00		A1	41	00			
0020	i	1A4	i	00	00	00	08	00	00	00	10	*******
0020	i	1AA	i	7F	FF	00	00	00	00	68	10	h.
0019	i	1B0	i	00	ØF	00	00	00	01			w)
0019	i	1CF	i	80	05	00	00	00				
0019	İ	1DC	i	02	00	00	39					9R./
0040	İ	21E	i	03	E8	37	45	22	06	01		7E"
0015	İ	244	İ	00	00	00	2A					
0039	İ	294	İ	04	0B	00	02	CF	5A	00		Z
0103	İ	305	İ	80								1.1
0099	1	309		00	00	00	00	00	00	00	AZ	*******
0100	1	320		00	00							
0100	Ì	324	I	74	65	00	00	00	00	0E	14	te
0099	Ì	333	Ì	00	00	00	00	00	00	16		
0100	İ	37C	İ	FD	00	FD	00	09	7F	00	14	

Results

- Effectively met project requirements
 - Technical ability to handle CAN-FD segments
 - Sequential Tx/Rx CAN messages (<5 mS)</p>
 - Implementation of key management protocols (J1939)
 - Generated key to handle encryption/decryption of messages; specifically, not OEM generated.
 TweetNaCl



Impact

- Strong safety applications to the vehicle industry
 - OEM and 3rd party manufacturers
 - Controllers can be used across vehicle platforms
 - Encourages business and innovation
 - Vehicle owners; improved safety

Conclusion

- Brings awareness to importance of digital security
- Novel approaches to encryption/decryption
- Abilities to transfer large amounts of data in little time

All images were created by researchers unless otherwise specified. Image 1 (KVaser). Additional resources are featured on sdmay23-15's website: <u>sdmay23-15</u>.sd.ece.iastate.edu