TATA ELXSI
engineering creativity

TATA

Gateway Architecture for Secured Connectivity and in Vehicle Communication

A Tata Elxsi Perspective

James Joy
Silvy Samuel
Vinu V S

Abstract

Keywords – Architecture, security, gateway, cryptography, Keys

As the electronics that goes into a car evolves at a rapid pace and the car progresses from an isolated unit to a networked/connected unit, cars are becoming increasingly vulnerable to malicious attacks. With the current advancements such as users being able to connect their personal devices like the tablet and cell phones to the car, access to cloud computing, car to car and car to infrastructure communications, there is nothing to stop anyone with malicious intent and with little computer-programming skills to gain access to the vehicle ECUs and take control of the vehicle. After gaining access, a hacker could control anything from, say, which song plays on the radio to start or stop the engine. Since all the ECUs usually share an unsecured CAN bus, cars thus require security measures similar to those implemented in e-commerce solutions and personal computing devices. Presently, car manufacturers are beginning to take steps to secure networks similar to those taken by the information-technology sector to lock down corporate servers. However, the current control units in vehicles are developed to address safety but not security requirements.

The objective of this paper is to provide an approach for secure automotive communication - both internal and external, by designing a central unit in the vehicle. A Smart Gateway ECU is proposed for this purpose, which would be based on modern cryptographic mechanisms to provide authentication, integrity and confidentiality mechanisms that shall solve the vehicular security issues. The Smart Gateway ECU consists of an external and an in-vehicle gateway. The external gateway interfaces with the outside world and the in-vehicle gateway interconnects the ECUs with the different vehicle networks. This module would support secure APIs for vehicle connectivity, which are governed by configurable security policies acting as a firewall controlling the access to the in-vehicle network. The Smart Gateway would additionally, handle secure key storage and management.

Introduction

Automotive systems are becoming increasingly dependent on embedded computers. The use of embedded computers provides better processing capabilities within the vehicle. The modern day luxury cars have multiple ECUs on board. During the introduction of electronic control in vehicles, isolated single board solutions were used. Later the scope changed to vehicle level solutions, with the help of distributed control units in the automotive network. The future trend is traffic level solutions, which are mainly addressed by the infotainment and telematics systems. As far as a customer is concerned, they need better performance, convenience, reduced cost and security for the system. Mobile devices connected to the vehicle enable OEMs to provide various utility applications that enhance the driving comfort. It also provides opportunity for an individual to explore the possibility of newer applications that makes the driving comfortable, informative and fun. But the downside is that an attacker could control the vehicle from "air" [1] [2]. Attacker, after a successful intrusion could try to read or write data from the vehicle network.

A wide variety of communication systems are available in today's automotive network, for different applications, ranging from body systems, engine control, driving assistances and safety systems to a wide variety of infotainment applications. Most of the communication systems are protected against different technical interferences. But these systems are mostly unprotected against the malicious attacks where the attacker tries to inject unauthorized packets into the network. The increased connectivity provided by the automotive systems, especially in the infotainment area is vulnerable to malicious attacks [12] [13].

The communication buses in the automotive network are classified as listed in Table 1, based on the technical properties and the application areas [9]. None of these automotive bus technologies provide an option for secure communication in the protocol definition.

Embedded security is one of the active areas within security [14]. Current automotive systems do not have inbuilt security mechanisms. Embedded security involves security against physical tampering, data security inside the device/ECU, authentication of the external devices connected as well as the ECUs, and the secure communication with external authentic devices. In the case of vehicle communication involving an external device, the device needs to be authenticated before the connection is accepted by the vehicle. The best way of providing security is through a public key cryptographic mechanism, which will address the secure communication with the device. Since the vehicle and the device are not trusted, it is very difficult to introduce a reliable authentication mechanism. The approach here is certificate based authentication. In the case of secure in-vehicle communication, the ECUs will be authenticated and secure communication enabled for required messages. Additionally, ECU data integrity would be ensured using public key cryptography.

The rest of the paper is organized in three sections, the first section deals with the security threats relevant to an automotive environment, the second part addresses security for external device connectivity to the vehicle, and the last part deals with the in-vehicle network security.

Com. system	Sub network	Event triggered	Time triggered	Multimedia
Buses	LIN	CAN	FlexRay	MOST
	I2C	VAN	TTP	D2B
	SPI	PLC	TTCAN	GigaStar
	K-Line		ByteFlight	USB
	UART			

Table 1: Automotive Bus Comparison

Security threats in automotive network

The different threat scenarios in the automotive network can be broadly classified as threats that occur due to the connectivity of the vehicle to the outside world and those that occur due to direct access to the in-vehicle network. Some of the attacks can be launched remotely without physical access to the vehicle, whereas other attacks require direct physical access to the vehicle and in most cases for prolonged duration. Additionally, some of these attacks require substantial time and costly equipments for successful execution.

Security is not part of the popular CAN protocol and it is difficult to introduce security in CAN as it is a proprietary protocol introduced by Robert Bosch. Here we are trying to address the security when the CAN network communicates with an external device [10] [11] and also in-vehicle security.

ECUs in the car are distributed over CAN or FlexRay network. These distributed ECUs communicate through messages. All ECUs on the CAN network receive all messages and the ECU will use messages that are relevant to it. The identity of the sender or receiver of the message is not reflected in the network communication. The message has its identity, and for that same reason anyone can inject any message into the network. The receiver of the message cannot distinguish between genuine messages and fake messages.

A sample of the different types of security threats that are possible in the automotive network is listed in Table 2 below:

Threats	Access Type	Interface
Man in the middle attack Intercept information sent to the vehicle, meaningfully modify and re-send it to the vehicle to control the car e.g. to start the engine, etc.	Direct physical/ Wireless	CAN/BT/WiFi/ GSM/ TMC/GPS/GPRS/ OBDII
Denial of service attack • Deleting encrypted premium content e.g. key storage file, or deleting some or all components of the OS • Reduce bandwidth by sending additional data • Break down the network by sending too much data	Indirect physical	Unauthorized apps from remote device or downloaded to the infotainment system
Replay attack • Replay V2V messages which were previously transmitted by other system entities • Replay CAN messages such as airbag ECU messages, door lock/unlock etc.	Direct physical/ Wireless	V2V (DSRC), CAN, OBDII
Collect private information Record messages transmitted by vehicles, especially safety beacons that report a vehicle's location, to track the vehicle's location and transactions, and infer private information about its driver and passengers	Short-range wireless	V2V
Unauthorized control of vehicle parameters Install program onto the car's CAN bus. Once on the network, the program could control every system from the windshield wipers, horn, rental fleet to brakes	Indirect physical	OBDII, CD, USB
False alerts V2V • Transmission of false hazard warnings • Tampered vehicles that forges messages to masquerade as an emergency vehicle to mislead other vehicles to slow down and yield TPMS • Report a tire problem tricking the driver to stop, who could then be robbed Injecting RDS-TMC traffic information signals as below • Standard traffic messages such as bad weather, full car park, accidents etc. • Close arbitrary roads, bridges, tunnels forcing the user to take detours • Security messages - such as terrorist incidents, bomb alert, etc. by sending corresponding code	Wireless	RDS, V2V, TPMS
Conceal location information Using GPS jamming devices, the GPS location information of the vehicle can be concealed for illegal activities or to prevent the owner of fleets from tracking the vehicle location	Long-range wireless	GPS
Loss of private/personal data • Copy privacy sensitive data such as keys or passwords • License tampering which will allow unauthorized access to protected content • Malicious application attempts to gain access to user private data (e.g. Email addresses, calendar information)	Indirect physical	Unauthorized apps from remote device or downloaded to the infotainment system
Tamper ECU data • Modify system parameters by modifying the calibration file and configure an invalid parameter • Change ECU configuration - Enable additional functionalities in the vehicle for financial advantage • Tampering the persistent database • Fake diagnosis operations	Direct physical	OBDII, CAN, JTAG
Bluejacking and Bluebugging • Send unsolicited messages over Bluetooth to Bluetooth-enabled device (Bluejacking) • Attack the Bluetooth interface to make phone calls, send messages, read/write contacts and calendar events, eavesdrop on phone conversations, and connect to the Internet (Bluebugging)	Short-range wireless	BT

Table 2. Security Threats in automotive networks

Topology

Vehicle level data exchange in automotive systems is facilitated by interconnection of different bus technologies. Gateways are used to transfer messages among each other, without taking into consideration different physical and logical operating properties. Usually Gateways provide protocol conversion, error protection and message verification. The so called 'Smart Gateway' provides the interconnection of all kinds of in-vehicle buses in the automotive network, and additionally act as an access point for other external devices to the vehicle [6]. The external devices include the tester and consumer devices. Access to external device is restricted by device authentication. Smart Gateways ares embedded computers capable of establishing secure communication with the external devices and ensuring secure in-vehicle communication among ECUs.

The proposed network topology is shown in Figure 1.

In the proposed topology, different kind of networks inside the vehicle are connected to a central gateway module - Smart Gateway. There can be multiple CAN and LIN networks, HSCAN from the chassis network, MSCAN from the body network, LIN, K-line from the sensors and many sub nodes. Additionally, MOST/Ethernet from the infotainment network [7] [8], and FlexRay from the safety critical X-by-wire systems are connected to the Smart Gateway.

The different threat scenarios listed in Table 2 above can be broadly classified as the those which occur due to connectivity of the vehicle to the outside world and those that occur due to direct physical access to the in-vehicle network. To handle these two kinds of threats the Smart Gateway ECU consists of an external and an in-vehicle gateway. The external gateway interfaces with the outside world and the in-vehicle gateway interconnects the ECUs in the different vehicle networks. Additionally, it contains a firewall which will restrict the data exchange with the external world and will act as a secondary security mechanism. The necessary modules inside the Smart Gateway are shown in Figure 1.

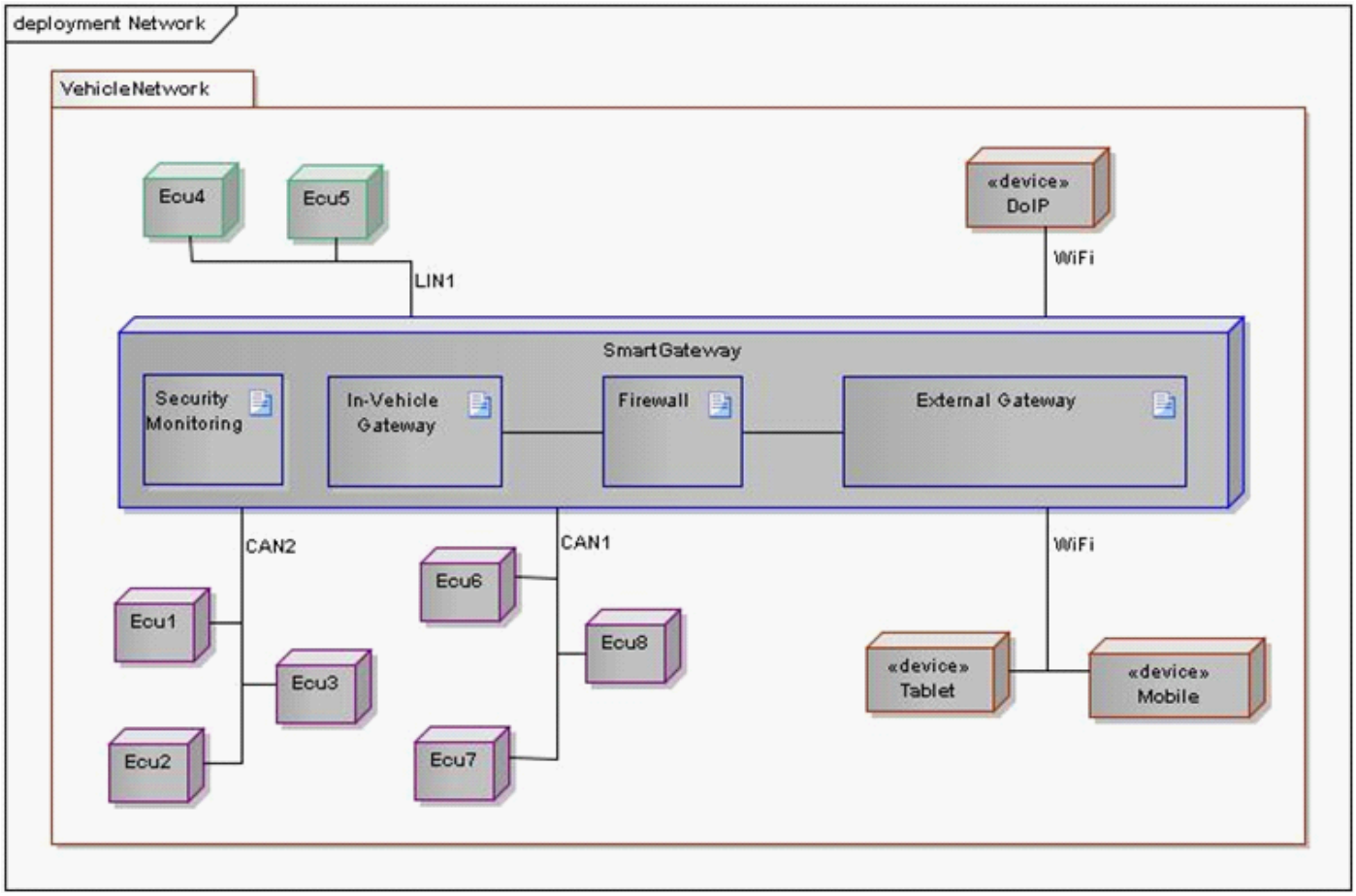

Figure 1. Network topology

Security of external communication

In an environment where wireless connectivity and third party mobile device is used, security is a cause of great concern. Secure Socket Layer (SSL) [3] can be used to provide security to the packets. SSL protocol uses asymmetric key cryptography to exchange keys and then uses symmetric key cryptography to exchange data. So the performance overhead is less. There are various versions of SSL available for embedded systems with the low computation requirement.

SSL is an industry standard for establishing a secure link between a server and a client. This secure link establishes integrity and security of the messages sent. This is a proven and widely accepted secure communication method. It is wise to use the proven security mechanism i.e. SSL in the vehicles.

The proposed architecture for external security depends on certificate based authentication and SSL based secure communication. The different modules inside the external gateway and the device are described in Figure 2.

The external gateway shall contain the authentication module which will provide certificate based authentication to the external connecting device. The secure communication module will provide secure data exchange between the external device and the vehicle.

The firewall will restrict the data exchange with the external world. It is not wise to accept all data/signals from the user applications in an authenticated external device. There can be external devices which have already been compromised and the firewall will act as a secondary security mechanism.

On the device side there will be a secure proxy module which will handle the authentication and secure communication between the Smart Gateway and the device. Secure_Apps are authentic applications signed by the OEM that can be installed in the device. These Secure_Apps could be any kind of application that requires an interaction with the vehicle. It could even be an infotainment application that includes standard infotainment features such as navigation, HVAC interface, audio and video applications. The audio and video applications in the device can communicate with the speakers and the other infotainment entities in the vehicle.

The proposed security framework involves authentication of the external device, data integrity during the communication between the device and the vehicle and tthe authentication of the applications downloaded and installed in the device.

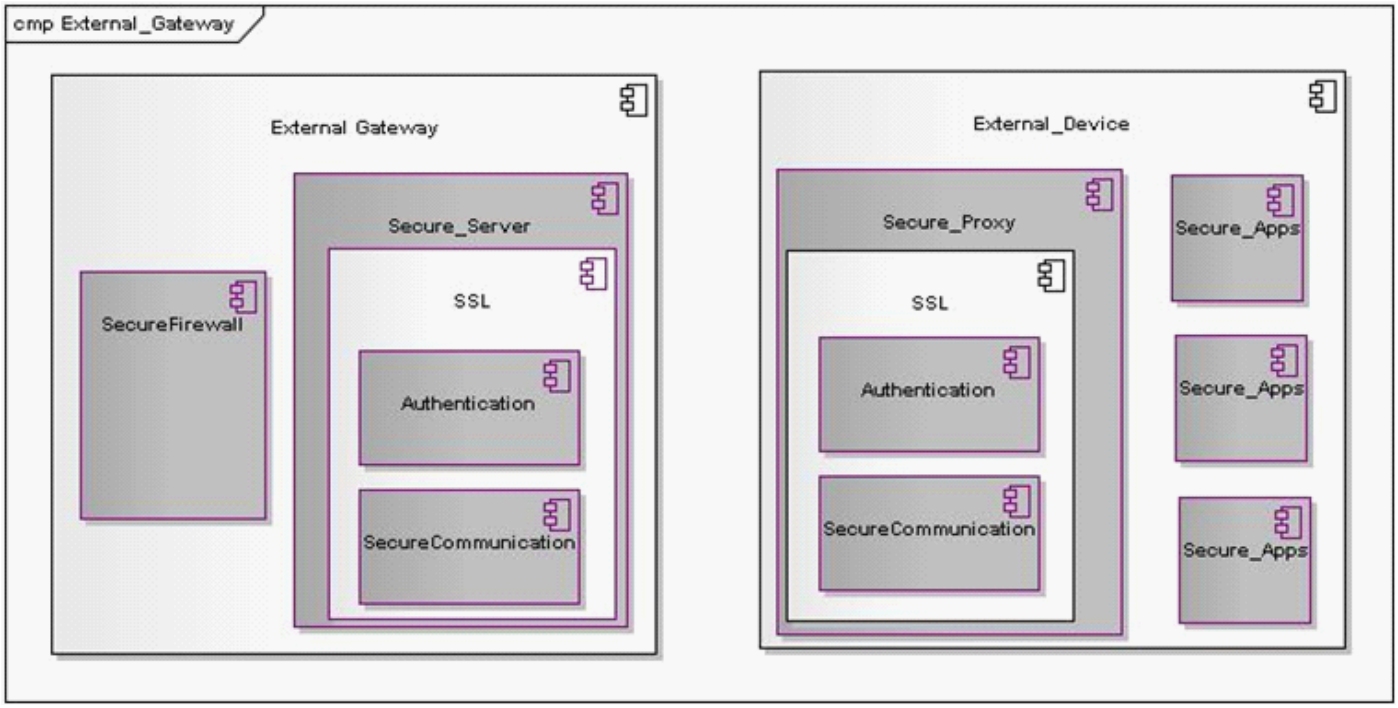

Figure 2. Security architecture - external gateway and device

Authentication

Secure identification of the device to the vehicle is a major cause of concern. Authentication makes sure that only valid devices are attached to the Smart Gateway. The certificate based security mechanism provides a better way of authenticating device with Smart Gateway. SSL has features to provide client authentication. Client certificate contains information that identifies the user and it can be used to authenticate him.

Integrity

Using WiFi connectivity, the automotive system enables attackers to access packets from the air and manipulate it. So the data should be exchanged securely when passed through air. SSL provides better security to packets sent through wireless channels. SSL provides data integrity by calculating digest of the message. At the receiver side digest is re-calculated and checked against the digest received. SSL uses HMAC for providing message authentication.

Application software security

A malicious application installed in the system can certainly break the functionality of the whole security system. In order to counter that attack, signature based methods are used. In the proposed framework all applications shall be signed by the OEM. The secure proxy will allow application connection only for applications signed by the OEM.

Security for internal communication

The main internal security threats are:

- Induction of false messages into the network
- Denial of service in the network
- Re-flashing of unauthorized code into the ECU
- Control the ECU through unauthorized diagnostics requests

The automotive networks are not meant for secure communication. These networks are hidden under the hood of the vehicle and the attacker needs prolonged physical access to these kind of attacks in most cases.

In this paper, we are addressing a solution to these security threats using the internal gateway module in the Smart Gateway. This is achieved by having a server security module in the internal gateway module and a client secure module in each ECU. This client-server combination will address the threats to a great extent. Finally a security monitoring module in the Smart Gateway will detect any further unauthorized access to the network and shall report to the anti-theft ECU. The details of this security solution are described below.

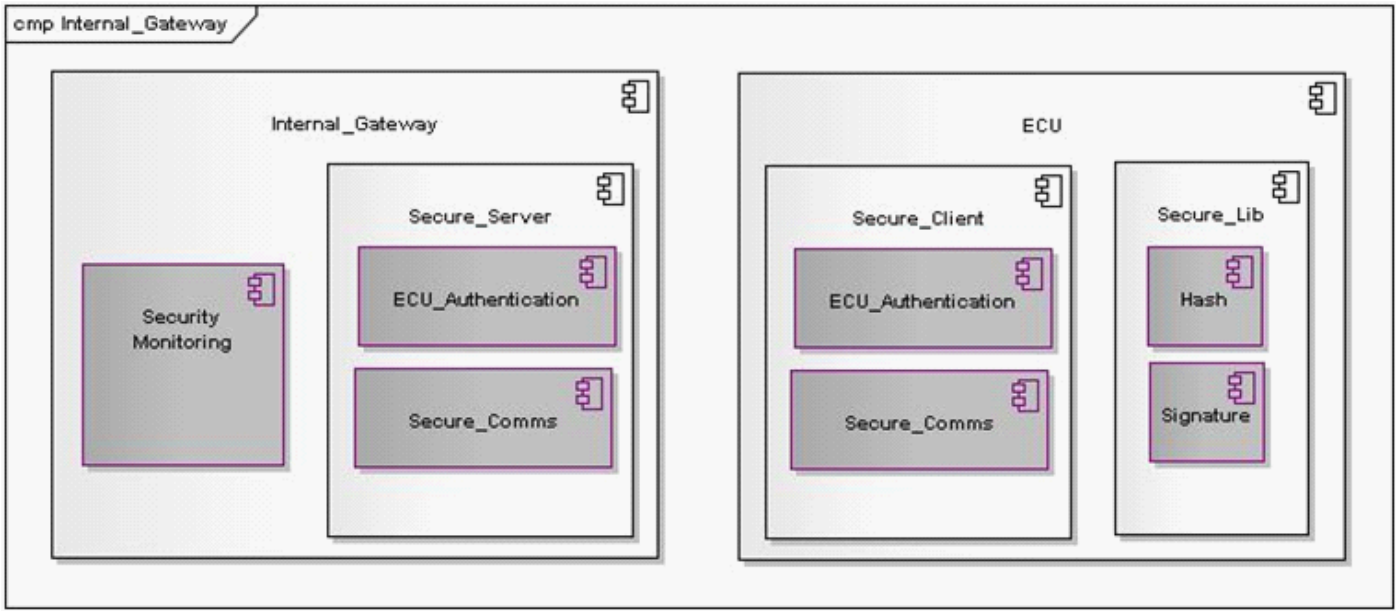

Figure 3. Security architecture - internal gateway and ECU

ECU authentication

Every ECU in the car is authenticated by the Smart Gateway via a nonce based challenge- response mechanism. After the authentication process, the gateway shall share the profile ID for the current driving cycle in an encrypted message. The selected profile shall be used by the secure communication module. So in every driving cycle, there will be a random selected secure communication profile distributed by the Smart Gateway.

Inter-ECU secure communication

All signals in the network need not be secured, the identified safety relevant signals are encrypted based on the security policy selected for that driving cycle. This is to minimize the overhead due to encrypting extra signals.

ECU data integrity

Every ECU might have configuration/ calibration data that need to be stored in the ECU, which needs to be protected against hacking.

For secure booting cryptographic checksum is used, where vendor uses private key to generate signature of the code that they want to deploy. The ECU has a public key, which is used to check the authenticity of the binary.

For secure ECU flashing, the OEM will sign the ECU software and the boot loader would verify this signature before the ECU software upgrade is flashed.

Security breach detection

There are numerous attacks possible in the CAN network, which cannot be avoided with the current CAN technology and our security solution. An attacker can send fake messages into the network since the CAN messages do not have sender or receiver identity in the message. CAN messages only have message identity. Similarly, an attacker can send diagnostic messages into the network if he is able to break the UDS/OBD security gate.

A software module in the Smart Gateway can monitor the network traffic and report any unexpected behavior. This module verifies

1. The periodicity of the messages
2. Validity of linked information with the message
3. Presence of diagnostic messages during non-diagnostic sessions
4. Presence of diagnostic messages during non-intended working conditions

The vehicle network security threat will be an additional input to the anti-theft ECU.

Conclusion

This paper presents an architecture for secure automotive communication - both external and internal, by using the Smart Gateway which consists of an external and an in-vehicle gateway and a firewall. The Smart Gateway handles authentication, data integrity and secure key storage and management for both external devices connected to the vehicle as well as for the network communication between ECUs.

References

1. Alex Wright. Hacking cars. ACM, 2011. Communications: 18-19.
2. Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, and Ivan Seskar. Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. In Proceedings of the 19th USENIX conference on Security (USENIX Security'10). USENIX Association, Berkeley, CA, USA, 2010. 21-21.
3. David Wagner and Bruce Schneier. 1996. Analysis of the SSL 3.0 protocol. In Proceedings of the 2nd conference on Proceedings of the Second USENIX Workshop on Electronic Commerce - Volume 2 (WOEC'96), Vol. 2. USENIX Association, Berkeley, CA, USA, 4-4.
4. Vipul Gupta and Michael Wurm. The Energy Cost of SSL in Deeply Embedded Systems. Technical Report, Sun Microsystems, Inc., Mountain View, CA, USA, 2008.
5. Helge Zinner, Josef Noebauer, Thomas Gallner, Jochen Seitz, and Thomas Waas. Application and realization of gateways between conventional automotive and IP/ethernet-based networks. In Proceedings of the 48th Design Automation Conference (DAC '11). ACM, New York, NY, USA, 2011. 1-6.
6. Pyungsun Park, Jaeil Jung, and Byounghweh Huh. Development of CAN-1394 Automotive Gateway System Using Designed Modular Software Stack. In Proceedings of the 2011 IEEE 35th Annual Computer Software and Applications Conference (COMPSAC '11). IEEE Computer Society, Washington, DC, USA, 2011 674-679.
7. Zonghua Gu, Zhu Wang, Shijian Li, and Haibin Cai. Design and Implementation of an Automotive Telematics Gateway Based on Virtualization. In Proceedings of the 2012 IEEE 15th International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops (ISORCW '12). IEEE Computer Society, Washington, DC, USA, 2012. 53-58.
8. Rolf Ernst, Gernot Spiegelberg, Thomas Weber, Herman Kopetz, Alberto Sangiovanni-Vincentelli, and Marek Jersak. Automotive networks: are new busses and gateways the answer or just another challenge?. In Proceedings of the 5th IEEE/ACM international conference on Hardware/software codesign and system synthesis (CODES+ISSS '07). ACM, New York, NY, USA, 2007. 263-263.
9. Marko Wolf, André Weimerskirch, and Christof Paar. Security in Automotive Bus Systems. escrypt GmbH, Bochum, Germany. Springer,
10. R. R. Brooks, S. Sander, J. Deng, and J. Taiber. Automotive system security: challenges and state-of-the-art. In Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead (CSIIRW '08), Frederick Sheldon, Axel Krings, Robert Abercrombie, and Ali Mili (Eds.). ACM, New York, NY, USA, 2008. Article 26 , 0 – 3
11. Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. Security Threats to Automotive CAN Networks --- Practical Examples and Selected Short-Term Countermeasures. In Proceedings of the 27th international conference on Computer Safety, Reliability, and Security (SAFECOMP '08), Michael D. Harrison and Mark-Alexander Sujan (Eds.). Springer-Verlag, Berlin, Heidelberg, 2008. 235-248.
12. Huaqun Guo, H. S. Cheng, Y. D. Wu, J. J. Ang, F. Tao, A. K. Venkatasubramanian, C. H. Kwek, and L. H. Liow. An Automotive Security System for Anti-theft. In Proceedings of the 2009 Eighth International Conference on Networks (ICN '09). IEEE Computer Society, Washington, DC, USA, 2009. 421-426.
13. Kerstin Lemke, Christof Paar, and Marko Wolf. Embedded Security in Cars: Securing Current and Future Automotive it Applications (1st ed.). Springer Publishing Company, Incorporated. 2010
14. Kerstin Lemke, Christof Paar, and Marko Wolf. Embedded Security in Cars: Securing Current and Future Automotive it Applications. Springer-Verlag New York, Inc., Secaucus, NJ, USA, 2005.
15. GENIVI http://www.genivi.org/
16. Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. USENIX conference on Security Berkeley, CA, USA, 2011

Contact us

For more information contact:
info@tataelxsi.co.in

About Tata Elxsi's Automotive services offerings

Tata Elxsi offers customized R&D services spanning across the product's lifecycle to automobile manufacturers and component suppliers. Our industry experience in working with leading OEMs, Tier1 suppliers, tool and chip vendors, makes us the preferred partner for system and sub-system design for the entire product lifecycle.

About Tata Elxsi

Tata Elxsi is a design company that blends technology, creativity and engineering to help customers transform ideas into world-class products and solutions.

A part of the $100 billion Tata group, Tata Elxsi addresses the communications, consumer products, defence, health care, media & entertainment, semiconductor and transportation sectors. This is supported by a network of design studios, development centers and offices worldwide. Key services include embedded product design, industrial design, animation & visual effects and systems integration. Tata Elxsi is a listed company and headquartered in Bangalore, India.

TATA ELXSI

engineering creativity