Securing In-vehicle Communication and Redefining the Role of Automotive Immobilizer

Constantinos Patsakis[1] and Kleanthis Dellios[2]
[1]*Universitat Rovira i Virgili Department of Computer Engineering and Maths, UNESCO Chair in Data Privacy, Av. Pasos Catalans 26 43007 Tarragona, Catalonia, Spain*
[2]*Department of Informatics, University of Piraeus, Piraeus, Greece*

Keywords: Immobilizer, In-vehicle Communication, Security, Authentication.

Abstract: Automotive conventional anti-theft devices fail to prevent from unauthorized actions against vehicles. Information technologies and evolved microelectronics are currently being developed and widely adopted in controlling many mechanical parts of the vehicles. One of the most common means of restricting access to unauthorized drivers is immobilizer. In current work we discuss some common vulnerability issues that vehicles and immobilizer technology confronts, leading us to propose a redefinition of its role in vehicle security and the physical vehicle environment. Our proposal meets current trends of IT and computer science in embedding systems in vehicles and if properly implemented, may provide more secure vehicles.

1 INTRODUCTION

Automotive industry is one of the largest economies and vehicles nowadays are improved in their functionality, performance, safety and comfort (Naver et al., 2009)(Fuhs, 2009). A vehicle is consisted of many embedded systems working together and communicating each other (Bonnick, 2001) creating an electronic environment that makes the vehicle operate as a platform entity. For this, CAN, LIN and MOST networks are being used. In addition, the vehicle is easier to be controlled and modified due to the different needs of a vehicle environment (Naver et al., 2009). Because of many vehicle act of threats in past, immobilizer technology (Heisler, 2002) has been invented and added as a security mechanism in modern vehicles. Its function is to prevent an engine from being ignited without the presence of the correct key. After their adoption, a significant decrease in vehicle thefts was observed, but in the past few years vehicle acts of threats have been increased again (ETP, 2004). Even if immobilizers deterred many thieves, several vulnerabilities in vehicles have become known, resulting to making them unable to protect a vehicle from being stolen (HS NewsWire, 2010). Thus, there is obviously a need for development of a new vehicle security mechanism.

The growing trend towards "computerizing" vehicles, by adding extra services that are offered by independent devices connected to the vehicle's infrastructure extend the attack layer making it prone to new more computerized attacks, like (Checkoway et al., 2011) or (Bailey, 2010). On the light of the recent research on vehicle security and current theft trends, big organizations and security firms are trying to make people aware of the dangers and find more secure solutions. Two very good examples are the US Department of Transportation, which recently issued a Request for Information and McAfee which issued an information bulletin (McAfee, 2011; FBO, 2011). It becomes apparent that not only vehicles become the next hacking platform, after smart-phones, but they can be attacked in cyber warfare situation, leading to huge problems.

The industrial approach towards in-vehicle communication is quite different from VANETs. In VANETs, correctly, the whole communication is governed by many cryptographic and authentication mechanisms, in order to secure the vehicle from outsider attacks. In the case of in-vehicle communication, the approach is quite different. Even though we are aware that a car that is about to be stolen will be attacked on its hardware infrastructure and communication systems, we haven't taken the proper countermeasures.

This work is an attempt to redesign the conventional security system, which is primarily designed to maximize the vehicle's performance and passen-

Patsakis C. and Dellios K..
Securing In-vehicle Communication and Redefining the Role of Automotive Immobilizer.
DOI: 10.5220/0004024302210226
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 221-226
ISBN: 978-989-8565-24-2

ger safety and vehicle's security as well. In this proposal, a more networked vehicle (Heisler, 2002) is being illustrated, where vehicle's control modules are being authenticated, on a new control unit, primary acting as a Trusted Third Party (TTP). In the proposed model, immobilizer is not circumvented but is being redefined, cooperating with the TTP module in the same centralized architecture creating an even more secure environment, more robust against many current attacks. This work has the following structure. In the following section we present the Immobilizer and general automative systems. Afterwards, we discuss current industrial standards and the security of the communications that they offer, whlile presenting some common vulnerabilities that current immobilizer technology confronts and vehicles vulnerability issues of IT interest. Then we present our proposal to vehicle security along with the possible protocol structure for its implementation. Finally, we summarize, giving some remarks for future work.

2 PRESENT IMMOBILIZER AND AUTOMOTIVE SYSTEMS

Vehicle has evolved into a complex device, as it is a mechanic machine controlled by numerous electronic units. This is achieved by the usage of power electronics, transforming the vehicle into an embedded platform, capable of controlling in large scale the mechanical systems of the vehicle and ensure its accurate function in real-time and continuity of tasks (Naver et al., 2009).

The role of automotive electronics is a major one, as they allow the vehicle control with great tolerance along with calibration stability (Bonnick, 2001). In addition, they create an embedded environment with many variable setups for a vehicle, electronics and motor as well. Micro-controllers are the main form of controlling an electronic vehicle system and they are the fundamental core of vehicle's computerised platform. Another major electronic control unit is the vehicle immobilizer, which is based on RFID Technology and cryptographic techniques. Until nowadays all vehicles are being equipped with an immobilizer unit that functions as the security system of the vehicle. The general principle is that immobilizer control module, needs to receive a transmitted signal from the factory's original keys of the vehicle owner in order to be activated. This is usually achieved by fitting an RFID chip inside the owner's keys. Unless the correct electronic signal is provided to the system by the ignition key, or a unique transponder or coded plug, the vehicle will not start and the engine will no be ignited(Naver et al., 2009; Bonnick, 2001; Heisler, 2002; Lemke et al., 2006).

As a result, when immobilizer operates, the vehicle's engine is not allowed to be ignited without first receiving the correct signal from the person trying to start it (Naver et al., 2009; Bonnick, 2001; Heisler, 2002; Lemke et al., 2006). More generic from an IT view, the immobilizer as a security mechanism will not allow the system to be functional until the very moment that the "certified user", owner of the vehicle's keys, has been authenticated. Immobilizers over the last years are tending to use more and more the so called "rolling codes", instead of "fixed codes". In the past, each time the key was used with the same transponder code, making vehicle vulnerable to replay attacks. In the case of rolling codes, a stream cipher is being used, so that each time the key is used, the transponder code changes. Sadly, as it has been shown by Nohl (Nohl, 2010) in many cases the encryption algorithms are poorly designed or poorly implemented, making vehicles easy to be stolen.

Finally, the immobilizer was invented, embedded in vehicles and became a "standard" vehicle part/module, when insurance companies confronted insurance issues, due to the state that vehicles were stolen. It became a necessity that vehicles, should have such an embedded security mechanism that could confront such acts of threat and obtain a more secure physical layer, as it was stated by the spokesperson for AUTOSAR S. Bnzel (eetimes, 2011). Apart from the creation of immobilizer, new standards of communication channels were also adopted both for sensors and control units and electronic automated on-vehicle diagnostics were added.

3 CURRENT STANDARDS AND VULNERABILITIES

The industrial standards that modern vehicles conform to, are a very good critirion of the supplied security of the information shared between vehicle's components. One of the wider adopted industrial standards in automotive industry is AUTOSAR (AUTOSAR), a framework for developing hardware components allowing their communication and interoperability. Currently, AUTOSAR is on the forth version, which was originaly released at the end of 2009. It is worth to notice that it is the first version of the standard refering to encryption, using the so-called Crypto Service Manager and the Crypto Abstraction Library. The aim of these two modules is to give an API to the manufacturers, which can be easily accessed from vehicle's software. In the standard there

is no definition of which cryptographic algorithms can be used, apart from MD5 and SHA which someone can infer from the text, what key lengths are supported, how passwords are generated (in case of public key algorithms). So we may deduce that all the previous versions are lacking the software support of standard encryption mechanisms from the framework. Cars that are more than 1-2 years old, the encryption of data and the use of authentication mechanisms was left on the manufacturers and whether they cooperate to encrypt the messages by the same way or leave it plaintext. In the new standard, despite the new additions and the disclosure of possible attack, data encryption has not become the default policy for data communication, while there is no referece for authentication with the rest of the system.

Two very common standards that are being used in vehicle hardware communication, are CAN (Controller Area Network) (CAN) and LIN(Local Interconnect Network) (LIN). CAN was introduced by R. Bosch in 1983, yet it is now covered by ISO 11898. CAN was originaly designed for automotive applications, but nowadays it has been widely adopted in the industry for device automation. On the other hand LINs are being used for smaller in vehicle systems and CANs' subnetworks. Both of these industry standards are low level protocols and are used as the main backbone for the communication of the hardware in the vehicle. Unfortunately, due to their nature, none of them supports encryption, making them prone to many attacks, as previously stated.

First types of attack in vehicles where methods such as breaking and entry, hotwiring, tampering or even towing and commonly used tools, in order to connect the battery source to the ignition, the so called Slim Jim tool to open locks and other formally known or unknown ways (Auto theft info, 2009; Car theft, 2009). As technology is evolving, all these ways have also evolved as well, so vehicles nowadays can be threatened through computerized attacks.

AUTOSAR highlighted vehicle security issues, as there is major necessity for secure programming of the Electronic Contol Units (ECUs), but still can be programmable only by authorized entities, the electronic immobilizer must always protect the vehicle from unauthorized driving via specific sets of cryptographic techniques. Furthermore, ECU software confronts the problem of existence of unstructured multiple unused functions or variants of data and also the secure diagnosis services.

As immobilizer units, RFID modules and generic anti-theft mechanisms vary in the way that each automotive vendor designs them for each vehicle, their application is based on specific set of cryptographic routines and services. A very good example of penetrating into these vehicles' security mechanisms by exploiting cryptographic primitives is the attacks on Keeloq algorithm, where a practical key recovery attack (Indesteege et al., 2008; Biham et al., 2007; Eisenbarth et al., 2008). Another important work by has proven that the encryption in RFID chipsets used in vehicles can be cracked without requiring direct contact, bypassing the security measures of a vehicle or even of the same immobilizer system (Bono et al., 2009).

Another vulnerability issue stems from an aftermarket product named RFID Zapper. It is an electronic device that has the capability of permanently deactivating passive RFID chips without damaging the chip that is being attacked. Since immobilizers are based on RFID authentication, it is possible to launch a DoS on them using proper hardware (RZ, 2010).

Another research revealed vehicle insecurity through remote exploitation and long dinstance vehicle control. Vulnerabilities where located in the OBD-II diagnostic port of the vehicles, via the infotainment system of the vehicle (accessories attacks such as Disk/Mp3 players, USB ports and iPod) and are indirect physical access methods. They also achieved short-range wireless access to the vehicles via Bluetooth, Remote Keyless Entry, RFIDs, WiFi, and Dedicated Short-Range Communications (DSRC). Also important vulnerability issues where shown through long-range wireless access attacks exploiting broadcast channels and addressable channels (Koscher et al., 2010),(Checkoway et al., 2011). In another attack scenario (Rouf et al. ,2010), researchers were able to to track cars and mislead drivers of potential problems in their vehicles, using as entry point the wireless tire pressusure monitoring system that modern cars have, which lack encryption mechanisms.

4 THE PROPOSAL

The first step is to redefine the immobilizer system, creating a safer environment for all the electronic modules and the vehicle as an entity. Current immobilizers have in IT terms, an "Accept all" policy towards almost all modules of a vehicle, because only immobilizer and the vehicle keys are the parts that are being authenticated and not the vehicle as an entity. Comparing to IT, no other security policy is applied or exists for the vehicle components. Therefore, there is a great need of adopting a "Deny all" policy towards all mechanical and peripheral parts of a vehicle could result to more secure vehicles and less acts of thefts. In order to implement this kind of IT security

policy, we introduce a Trusted Third Party (TTP) that authenticates each vehicle's module. The TTP can be installed on the MCU of the vehicle so that all network traffic can parsed from it.

Module categorization is crucial to this security model for the vehicle's functionality. The categorization is being implemented because a vehicle has many ECUs and safe usage of the vehicle and safety of the user might be affected. The categorization of the automotive modules should be based on the peripheral topology and are divided in Primary and Secondary systems. Every time that a malfunction is discovered in a Secondary module the fully usage of the vehicle must not be affected and the vehicle's mechanical usability should not be suspended, yet the secondary module will only be deactivated and any packet traffic from it shall be blocked, as this might be caused by an attacker. On the other hand, if a Master Module is not authenticated, then it will trigger in this case the Immobilizer to halt any vehicle usage. The necessity of this categorization is because vehicles are designed for long-term use and their parts suffer a lot from pressure, usage, collisions, resulting to many minor or serious malfunctions through the pass of time. It is therefore a functionality issue for example to let the vehicle moving, even if the MP3 player is broken or even if the power windows are not working. In another case, the vehicle should not allow any further use if its steering wheel confront an electrical/electronic problem.

Moreover, the vehicle is provided with a built-in database for different user profiles e.g. driver, co-driver, vehicle technicians/mechanics, parental control for children/elder person, other persons. Each profile provides the driver/user with a different setup and use of the vehicle. So that a technician/mechanic cannot drive the car for more the 20km, or with parental control we may allow a young driver use the car in a certain radius away from home or restrict the use of the vehicle in certain areas. Moreover, we may allow a driver use the vehicle in pre-assigned routes, or even enable some functionalities like mp3 player, GPS, A/C for certain drivers. Of course each user may be authenticated either by biometrics or by keys, e-keys etc. It is obvious that this categorization goes beyond offering advanced infotainment experience on the vehicle. The scope of this categorization is to provide different access level to possible users of the vehicle.

The difficult part is the upgrade of today's vehicle's component/module in order to be easily software or firmware, updated and/or upgraded, only by authorized resellers/sources via the TTP. Immobilizer in this security model acquires a more crucial role for the vehicle, as it can be triggered by more events that were not covered up to now and its role becomes more crucial as its function is needed for triggering the engine's shut down in case of a malfunction or violation is detected.

The TTP will control all primary modules. The detection, identification and authentication of all modules will be made by the TTP. Identically, the primary modules will control all secondary modules attached to them. Between Primary modules and TTP there will be a firewall in order to protect TTP from attacks launched by unauthorized modules or maliciously injected code on authorized modules. Between TTP and ICM there will be two party communications and an application firewall. The TTP must be designed in a way that sensors can adapted and linked with in the future, so as to implement further security checks in tampering vehicle body-train and motor engine or for future improvements of the security system. During the process of initialization we have a mutual identification of all modules with TTP. Moreover, vehicle's users will be identified and authenticated automatically through the different access levels that are stored in system profiles. System profiles are responsible to enabling and disabling primary and secondary modules for a given period of time or use, if authentication is successfully completed. In case that a severe malfunction is detected in primary modules, TTP triggers immobilizer with a shut down message. Secondary modules are deactivated and incoming data is blocked.

The structure protocol that we propose is very close to SSL with mutual authentication, when it comes to vehicle initialization, and Kerberos like, whenever a module wants to access another module. Whenever the vehicle is turned on, the following exchange of messages is made with each module. The Immobilizer sends a iniatilize authethication message to the module. The module sends the Immobilizer the ciphers supported, data compression methods, random data (RD_1) and the access list.

Firstly, the Immobilizer examines the privileges of the module and whether the access requested is legitimate, depending on the rights of the user that has been authenticated, the requested access will be granted. In case of full restriction, the communication is terminated. If the module has the rights to make a request, the Immobilizer replies with the selected ciphers, data compression methods, an assigned session Id and some random data (RD_2). The immobilizer appends its certificate and, a chain of certificates beginning with the certificate of the certificate authority (CA), if it is not assigned from a root authority. The module chetacks the Immobilizer certificate and

sends its own, followed by a chain of certificates beginning with the certificate of the CA, if not assigned from a root authority. Immobilizer checks them and replies using a mutually generated key K, from RD_1 and RD_2, encrypting the list of the keys that are going to be used, the period of their validity and the list of allowed access. The module replies with an encrypted hash of the previous messages with key K. The server replies with an encrypted hash of all previous messages with key K.

Immobilizer acts as a ticketing server, issuing tickets to each module for communication with other modules, which are valid only for a random period, subject to exchanged messages, in order to prevent attacks on static period of time and to control the communication and the access of each module. To allow communication of $module_1$ with $module_2$, the following procedure is followed. $module_1$ sends a nonce and request for communication with $module_2$, for access list AC, encrypted with key K_1. The immobilizer checks whether $module_1$ has the right to communicate $module_2$ and using AC. In this case, it creates a random number T, the tickets to be exchanged, a random number r, and key $K_{1,2}$. Then it sends $module_2$ the message $E(r,T,module_1,K_{1,2},AC)_{Pr_I}$ encrypted with key K_2. $module_2$, decrypts the message using Pub_I and K_2 and if it is available for use on that period responds with $H(r,T)$ encrypted with key K_2. Immobilizer sends to $module_1$ the message $E(nonce,T,K_{1,2})_{Pr_I}$ encrypted with key K_1. $module_1$, decrypts the message using Pub_I and K_1 and obtains T and $K_{1,2}$. $module_1$ sends $module_2$ messages encrypted with key $K_{1,2}$, appending each time the current value of T at the end. $module_2$ decrypts the messages using key $K_{1,2}$ and checks the requests against AC, if any of them exceeds them, then $module_2$ issues an alarm. For each received message value T is decreased. K_i is the key that immobilizer has issued to $module_i$, Pr_I is the private key of the Immobilizer and Pub_I is the public key of the Immobilizer.

In order to circumvent these measures one might try to install a "new" Immobilizer system, trying to initialize the ignition of the engine with his prefered policies. To protect the vehicle from such attacks, we must change the policy of the modules. Therefore, on initial configuration of the vehicle, the modues access from Internet the first hardware profile and store the Immobilezer's "fingerprint". In case the Immobilizer changes, the modules temporarily authenticate it, demanding access to the Internet in order to check for the afforementioned update in the profile of the vehicle, issuing an alert in case the profile is does not contain such alternation. Moreover, storing the fingerprint of the immobilizer prevents any disclosure of important keys from possible future hardware attacks.

5 CONCLUSIONS

When we are stepping from IPv4 to IPv6 and from http to default https on many web servers in order to provide advanced security to end users, it is at least irresponsible to leave such vital and widely used parts of our everyday lives, without further modifications on network layer. It is not coinsidencial that even after making immobilizers a default security system in most of the vehicles, especially in cars, they are still being stolen. This fact is proving that conventional anti-theft vehicle systems fail to prevent unauthorized usage. It is obvious that new methods should be developed to enhance current security status.

The scope of this work is to propose a way to improve vehicle's physical layer security by combining automotive vendors technology and information technology knowledge. In this proposal, the role of immobilizer is redefined and is being used as a trigger mechanism, while an advanced TTP undertakes the complete role of the security mechanism. Firewalls are applied in order to prevent electronic attacks on the vehicle from multimedia applications, vehicles ports or even unauthenticated and malicious hardware. Moreover, the in-vecicle communication is encrypted and provides authentication methods to its modules. The proposed security model can also provide different profiles database for the authenticated user, preventing malicious attacks and acts of threat against the vehicle from privilege escalation of potential drivers/users. The illustrated protocol is only given to provide a general idea of the proposed structure and how different and more secure it can prove to be, compared to the current solutions for in-vehicle communication.

Based on current proposal, many extensions may be implemented. One may extend user authentication using biometrics measures instead of portable, but easy to lose credentials such as keys, e-keys etc. Moreover each vehicle can have a profile on the manufacturer or on a trusted company which is updated every time a part is changed. This way, plugging devices in order to compromise vehicle's security can be traced and prevented. The TTP can be designed to allow Internet or 3G connection so that any kind of sudden or strange changes on the vehicle's profile may instantly trigger alerts, enabling further security and proactive measures to be taken, even on road, without affecting vehicle's stability and driver's safety.

DISCLAIMER AND ACKNOWLEDGMENTS

Constantinos Patsakis is with the UNESCO Chair in Data Privacy, but he is solely responsible for the views expressed in this paper, which do not necessarily reflect the position of UNESCO nor commit that organization. This work was partly supported by the Spanish Government through project CONSOLIDER INGENIO 2010 CSD2007-00004 “ARES”.

REFERENCES

Auto theft info, http://www.auto-theft.info/Statistics.htm

D. Bailey, “War Texting: Identifying and Interacting with Devices on the Telephone Network”, Black Hat, USA 2010.

E. Biham, O. Dunkelman, S. Indesteege, N. Keller, B. Preneel, “How to Steal Cars - A Practical Attack on KeeLoq”, Crypto 2007.

A. W. M. Bonnick, “Automotive Computer Controlled Systems, Diagnostic tools and techniques”, Butterworth-Heinemann, 2001.

S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, M. Szydlo, “Security Analysis of a Cryptographically-Enabled RFID Device”, USENIX Security, July 31-August 5, 2007.

Car theft, http://www.car-theft.org/theft-methods

S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, “Comprehensive Experimental Analyses of Automotive Attack Surfaces”, USENIX Security, August 1012, 2011.

EE Times, http://www.eetimes.com/design/automotive-design/4213069/AUTOSAR-architecture-expands-safety-and-security-applications?pageNumber=0

T. Eisenbarth, T. Kasper, A. Moradi, C. Paar1, M. Salmasizadeh and M. T. M. Shalmani, “Physical Cryptanalysis of KeeLoq Code Hopping Applications”. Ruhr University of Bochum, Germany http://eprint.iacr.org/2008/058.

Electronic Theft Prevention, The Immobilizer Project, report from Larmtjanst, Swedish insurance Federation Company, 2004.

Federal Business Opportunities, Cyber security and Safety of Motor Vehicles Equipped with Electronic Control Systems, Solicitation Number: DTRT57-11-SS-00007 https://www.fbo.gov/index?s=opportunity&mode=form&id=40c0c2730b334df090dba322a61e956f&tab=core&_cview=0

A. E. Fuhs, “Hybrid Vehicles and the Future of Personal Trensportation”, CRC Press, Taylor & Francis Group, 2009.

H. Heisler, “Andvanced Vehicle Technology”, 2nd ed. Butterworth-Heinemann, 2002.

Homeland Security News Wire, http://www.homeland securitynewswire.com/ car- immobilizers- no- longer-problem-car-thieves.

S. Indesteege , N. Keller , O. Dunkelman , E. Biham , B. Preneel, “A practical attack on KeeLoq”, EUROCRYPT’08 Proceedings of the theory and applications of cryptographic techniques 27th annual international conference on Advances in cryptology, 2008.

K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security and Privacy, Oakland, CA, May 16-19, 2010.

K. Lemke, C. Paar, M. Wolf, “Embedded security in cars, securing current and future automotive it applications”, Springer-Verlag, 2006.

McAfee, “Caution: Malware Ahead”, http://www.mcafee.com/ us/ resources/ reports/ rp-caution-malware-ahead.pdf

N. Naver, F. Simonot-Lion, “Automotive Embedded Systems Handbook”, Industrial Information Technology, CRC Press, Taylor and Francis Group, 2009.

K. Nohl, “Car Immobilizer Security”, escar 2010, Bremen, November 2010.

RFID-Zapper project: https://events.ccc.de/congress/2005/static/r/f/i/RFID-Zapper(EN)_77f3.html

Automotive Open System Architecture, AUTOSAR, http://www.autosar.org/

LIN Overview, “Lin Concept”, LIN Administration, http://www.lin-subbus.org/index.php?pid=5&lang=en&sid=7978e50790ccd16bb12bf6307eae5a74

Bosch specification of CAN-bus, http://www.semiconductors.bosch.de/media/pdf/canliteratur/can2spec.pdf

I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar , ”Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study,” in Proceedings of the 19th USENIX Security Symposium, Washington DC, August 11-13, 2010