ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Adaptive Cruise With Anti Steering Control Using WSN

Prasanna.D, Kalaiselvi.B

Department of Electronics and Communication Engineering, Bharath University, Chennai, Tamil Nadu, India

Department of Electronics and Instrumentation Engineering, Bharath University, Chennai, Tamil Nadu, India

ABSTRACT: In this project we design the autonomous and manual vehicle system using the embedded system with wireless communication. In this system we provide high security by using the communication like automatic for RF and manual. Using the RF system we can control the vehicle remote via and using obstacle sensor we can find obstacle in the path. Society is becoming increasingly dependent on embedded computing and sensor technology to enable complex networks of autonomous systems, such as robots, unmanned aerial vehicles (UAVs), self-driving cars, and unmanned underwater vehicles (UUVs). Smart Just Drive for Automotive using embedded blue tooth is designed to provide comfortable feel to the user or passenger to check the vehicle status by reading different vehicle parameters like fuel levels, engine temperature etc., and remote by using Smart mobile with Bluetooth Connectivity. This is an inexpensive device which reduces the problem associated with anti- theft control as well. In this paper, we present an automotive security system to disable an automobile and its key auto systems through remote control when it is stolen. It hence deters thieves from committing the theft.

KEYWORDS: Automotive, CAN Bus, ECU, MEMS, Accelerometer, Navigation control module (NCM), 3333 Engine control module (ECM), and 333 Electronic brake control module (EBCM).

I. INTRODUCTION

Automobile in-vehicle networks have historically been isolated from attackers due to the limited access possibilities, but with the advent of wireless Internet-based connectivity between the vehicle and its surroundings, this is about to change. The introduction of a wireless gateway as an entry point to the in-vehicle network allows for remote interaction with vehicle firmware, even when the vehicle is running. This allows remote diagnostics and thus, vehicle owner's donors have to drive to a service station to get their car diagnosed. Moreover, firmware updates can easily be applied to thousands of vehicles simultaneously, instead of interfacing each vehicle through the on-board diagnostics (OBD) module, thus removing the need for attaching and detachingcables.In addition, vehicle-to-vehicle and vehicle-to-roadside communication, inter-vehicle communications systems allow vehicles to alert each other of changing weather conditions and to obtain area information from roadside stations.

However, the new technology also introduces new safety and security issues for the manufacturer to consider; cyber attacks on vehicles are introduced. We dense cyber attacks as attacks that target the vehicle network. An attacker could, for example, use the firmrmware update feature to inject malicious code into the vehicle network while the vehicle is running. As an illustration, consider the case of a speeding vehicle that hits the face of a rock. This incident is either caused by the driver itself, or by vehicle malfunction or physical tampering. If the brake wire is found to be cut, the cause of the accident is most certainly an act of physical tampering, and a criminal investigation needs to be initiated to bring the responsible to a court of law. Current in-vehicle network produces data necessary for the operation and maintenance of the vehicle, and to protect the vehicle from safety-related incidents.

However, when an intelligent attacker is introduced, there is a need to produce data that can reveal both the presence of malicious code, and provide evidence that will aid investigation of a cyber attack. In this paper, we state a set of requirements for digital forensic investigations of cyber attacks on automobile in vehicle networks. We analyze the current in-vehicle network structure, including node layout and external interfaces. Based on the analysis we derive an attacker model and dense attacker actions.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

II. HARDWARE ARCHITECTURE

A. The In-Vehicle Network

The network in the vehicle consists of nodes, gateways, and buses. A node is an Electronic Control Unit, or ECU, Which is connected to the bus? The bus is the shared data transfer media, e.g., copper cables. The buses and the nodes form a network. Data may be transferred from one network to another through a gateway. The ROM memory contains the firmware that is executed on the ECU. Each ECU is responsible for the functionality of a certain area in the vehicle. For example, one ECU is responsible for the head lights system, and one ECU handles the driver door functionality (e.g., lock and window). For more complex functions such as the engine system, a number of Excusers co-operating. Each ECU also has a RAM data area for parameter storage (e.g., which lights are turned on etc.).There are different network types in an in-vehicle network [20][21]:

Controller area network (CAN), local interconnect network (LIN), and media oriented systems transport (MOST). CAN is the most common network in a vehicle today. There are often several CAN networks, e.g., power train and comfort CAN [22][23]. LIN is a communication protocol used for non-safety critical sensor/actuator systems where CAN is too expensive or not suitable. Communication in LIN is based on a master-slave architecture, where the master is connected to the CAN bus and relays traffic between the CAN and the LIN networks [23]. The MOST protocol is used to carry audio and video information. This network often employs a ring topology with optical fiber for sending/receiving data in a master-slave fashion. The master is connected to the CAN bus and relays traffic between the CAN and MOST networks [20][21].

B Administrative Functions

Two common administrative functions that exist for vehicles are diagnostics and firmware updates. Diagnostics is used to eject single data parameters in nodes [24], and is used for reading node status, such as the passenger door is locked, or controlling node activity (e.g., unlock the passenger door) by writing node status. Diagnostics is usually done through the OBD interface and can be performed.

Firmware update is the process of re-cashing the memory of the ECU to install new firmware, e.g., in the case of vehicle functionality problems [9][10]. The new application binary is transmitted on the bus, and the target ECU ashes the binary to its ROM and reboots. The well-known security design principle defense-in-depth still applies but must be adapted to the in-vehicle network setting. In this paper we discuss five layers of defense-in-depth: prevention, detection, deflection, countermeasures, and recovery. We therefore focus on intrusion attacks and analyze what methods an attacker can use to read and write data from and to the ECUs.An attacker that wants to elect the in-vehicle network and the ECUs has three means of doing this. The three actions an attacker can perform are diagnostics requests, low-level requests, and update the node rewire. Sending diagnostics queries (SD): An attacker can send read or write requests to get or set certain parameter values in an ECU. Sending low-level requests (SL): An attacker can send low-level read or write requests to read or write the byte value of a certain memory address. Performing _rewire updates (FU): An attacker can update an ECU with new rewire through re-hashing. Thus, an attacker can change the functionality of an ECU to perform malicious acts.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

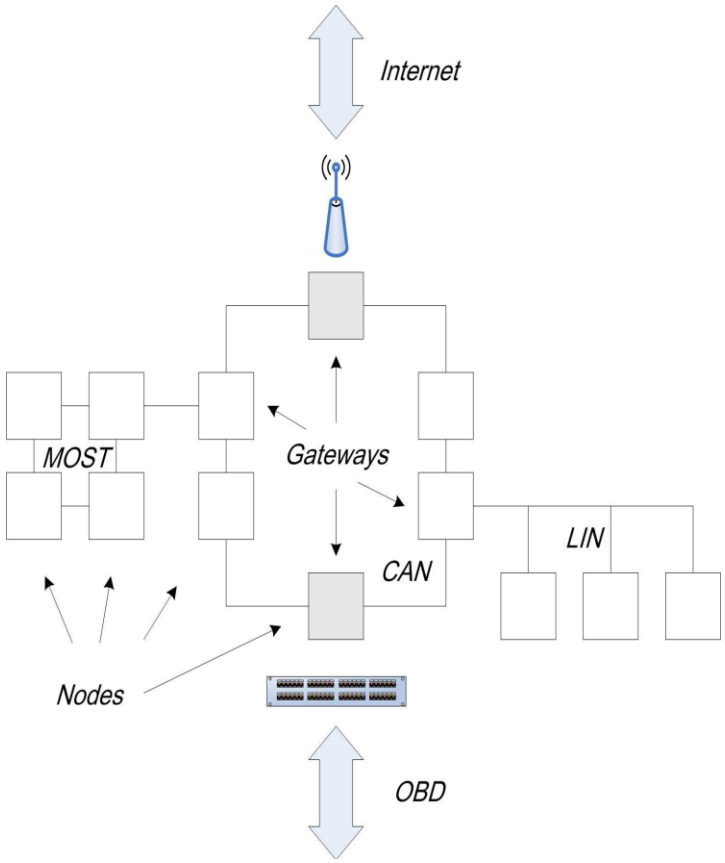


Figure 1: An in-vehicle network consisting of the CAN, LIN, and MOST networks, and two external

III. THE NEED FOR SECURITY

Current in-vehicle networks primarily meet safety requirements. They are thus designed to withstand failures caused by non-malicious and inadvertent flaws which are produced by chance or by component malfunction. Deployed protection mechanisms are therefore realized by means of fault-tolerance techniques, such as redundancy, replication, and diversity. Since the in-vehicle network historically has been isolated, threats other than those against the safety of the vehicle have not been considered. Therefore, protection against threats originating from intelligent attackers (i.e., security protection) has not been included in the requirements or the design of such networks. Alongside the emerging trend of allowing external communicating parties to interact with the in-vehicle network, an imminent need for security arises. There exist a number of security best practices; however, since the in-vehicle net-work is a non-traditional network in the sense that it consists of resource-constrained embedded computers and the traffic patterns differs from IP-networks, a new set of best practices for such networks must be developed.

B. Prevention.

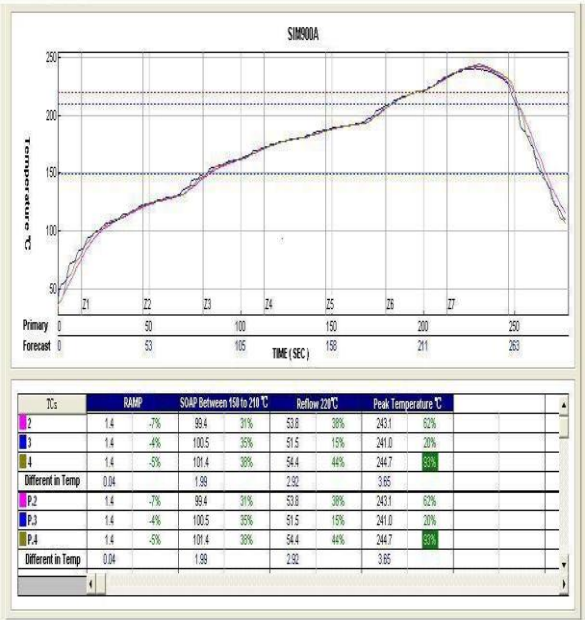
Prevention is necessary to allow only authorized accesses to interact with the vehicle and within the vehicle. For external communication, proper authentication mechanisms are essential to prevent attackers from sending bogus data or accessing services in the vehicle. In addition, access control and firewalls are necessary to prevent unauthorized accesses and intrusions to the vehicle. For communication within the vehicle, i.e., communication between the embedded computers in the in-vehicle network, proper authentication mechanisms are important to prevent attackers from hijacking an embedded computer or sending false data. The communication protocols in the in-vehicle network have currently no security protection and must be redesigned to incorporate several security features. To determine which ECUs to protect and prevent access to a classification based on safety-security characteristics should be consulted.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015



TCs	RAMP		SOAP Between 150 to 210 °C		Reflow 220°C		Peak Temperature °C	
T2	1.4	-7%	99.4	31%	53.8	38%	243.1	62%
T3	1.4	-4%	100.5	35%	51.5	15%	241.0	20%
T4	1.4	-5%	101.4	38%	54.4	44%	244.7	83%
Different in Temp	0.04		1.99		2.92		3.65	
P.2	1.4	-7%	99.4	31%	53.8	38%	243.1	62%
P.3	1.4	-4%	100.5	35%	51.5	15%	241.0	20%
P.4	1.4	-5%	101.4	38%	54.4	44%	244.7	83%
Different in Temp	0.04		1.99		2.92		3.65	

Figure 1: Prevention diagram of an in-vehicle network system

C. Detection

Detection is imperative to find attacks on the vehicles and in the in-vehicle network. For external communication, the wireless gateway on the vehicle must incorporate an adequate logging mechanism and provide intrusion detection capabilities. Unauthorized access attempts to services and intrusion attempts to the vehicle must be detected and properly logged by an intrusion detection system. For the in-vehicle network, a lightweight detection and logging mechanism must exist. It is imperative that this mechanism is lightweight since most communication on this network has real-time constraints. Unauthorized access attempts and intrusion attempts to the embedded computers must be detected and logged by a dedicated detection process.

D.PROBLEM DEFINITION

In this section, we formulate a dentition of the problem and the design goals for a complete solution for in vehicle network digital forensic investigations. In addition, we present the considered attacker model, based on terms presented by Howard and Longsta in the CERT taxonomy. We dense an event as an action which is intended to result in a change of state of a selected target. We further a security violation as an event that violates security policy rules, and an attack as a series of steps, where one or more events are included, taken by an attacker to violate the security policy.

IV. DESIGN GOALS

To properly perform a digital forensic investigation the necessary data must be present. A method to detect events in the vehicle must be present. To perform a digital forensic investigation, an alert about a security violating event must have been triggered to provide reason to initiate the forensic investigation. Data to answer the questions who, what, where, when, and why must be produced in the vehicle. During the forensic investigation, this data must be available in the ECUs for an investigator to extract the necessary information when needed. Information about the current state (e.g., firmware versions)in a vehicle must be available and stored in a secure location. To detect whether the vehicle has been tampered with, the extracted data must be compared to the original data.

4.1 Attacker Model

In our attacker model, we assume that an attacker can access the in-vehicle network from either the Internet interface or the OBD interface. We further assume that the attacker can perform the actions presented in , e.g., inject, modify, and

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

replay messages on the bus as shown in. Moreover, we assume that the attacker can install software, and delete potential logs to hide its presence. We assume that an attacker after a successful intrusion attempts to either read from, or write data to the ECUs. By reading data, an attacker can attack congeniality (secret keys) and privacy (read private driver information).By writing data, an attacker can attack integrity (change functionality of ECUs) and availability (disable ECUs). We therefore focus on intrusion attacks and analyze what methods an attacker can use to read and write data from and to the ECUs.An attacker that wants to eject the in-vehicle network and the ECUs has three means of doing this. The three actions an attacker can perform are diagnostics requests, low-level requests, and update the node firmware. Sending diagnostics queries (SD): An attacker can send read or write requests to get or set certain parameter values in an ECU. Sending low-level requests (SL): An attacker can send low-level read or write requests to read or write the byte value of a certain memory address. Performing firmware updates (FU): An attacker can update an ECU with new firmware through re-cashing. Thus, an attacker can change the functionality of an ECU to perform malicious acts.

V. REQUIREMENTS FOR A DIGITAL INVESTIGATION

The present vehicle network is primarily designed to support operational safety and maintenance considerations. As discussed earlier, this is not sufficient for protecting against cyber attacks. We use the design goals along with the attacker model to derive a set of requirements for supporting the digital investigation. The set of requirements is divided according to the design goals and are denoted: Event detection requirements, Forensic data requirements and State information requirements.

5.1 Event Detection Requirements

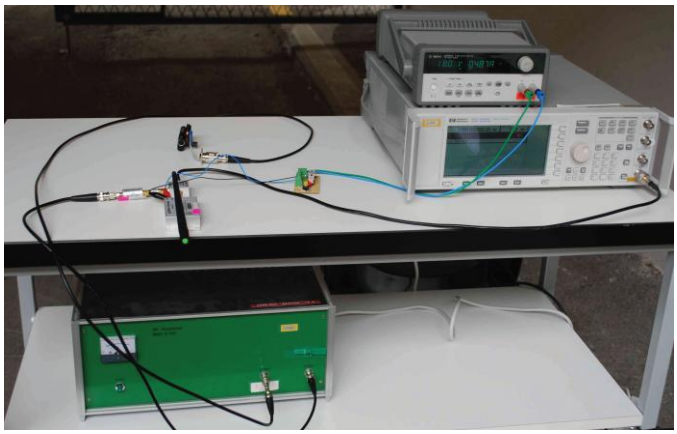


Figure .2(a) Key side.

To detect an event at an early stage it is necessary to introduce a detection mechanism to the in-vehicle network. The event detection requirements address what devices need to be present to detect and alert the appropriate authority that a security violation has been detected. A model-based detection system [4] maintains a list of allowed communication patterns and alerts when prohibited events occur. Also, the alert data is used together with the event data to aid investigation. In addition, there is a need for a storage device and a device. (>50K$) cars, 1 minivan and 2 cars in the compact class(<30K$). We had two different models for only two of the tested manufacturers. During the evaluation of the 10 different PKES systems, we observed that all of them differ in their implementation. We also noticed that even if they rely on the same general idea and similar chips the overall system behaves differently for each model 7. The differences were found in timings (as shown below), modulation and protocol details (e.g., number of exchanged messages, message length). Only the aftermarket system was obviously not using any secure authentication mechanisms. When possible, on each car we measured the distances for the relay, the maximum acceptable delay and the key response time and spread. In this section we describe different attack scenarios and discuss the implications of relay attacks on PKES systems. Common Scenario: Parking Lot. In this scenario, the attackers can install their relay setup in an underground parking, placing one relay antenna close to the passage point (a corridor, a payment machine,

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

an elevator). When the user parks and leaves his car, the Passive Keyless Entry confident that his car is locked (feedback from the car is often provided to the owner with indicator lights or horn).Once the car is out of user's sight, the attackers can place the second antenna to the door handle. The signals will now be relayed between the passage point and the car. When the car owner passes in front of this second antenna with his key in the pocket, the key will receive the signals from the car and will send the *open* command to the car.

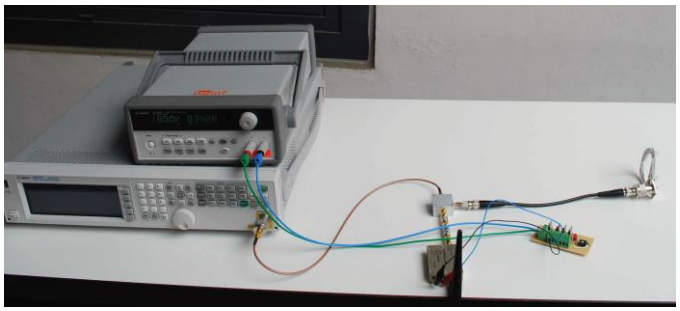
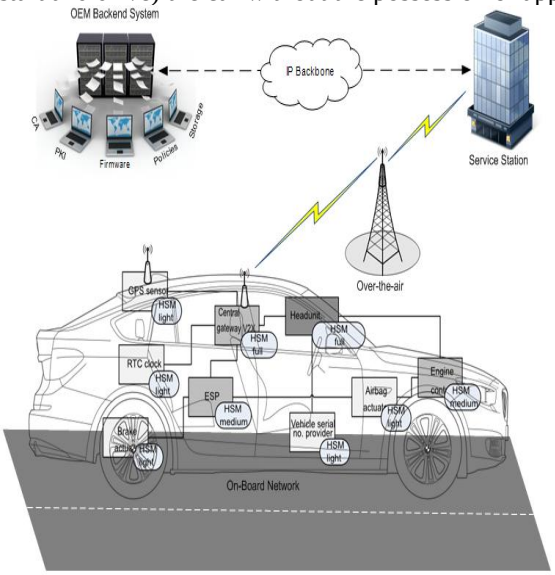


Figure.3 (b) Car side.

The results show large differences between different car models. The key response standard deviations vary from 4 to 196 μs, and the maximum spread - from 11 to 436μs.These values show that the current implementations exhibit large variance.

VI. IMPLICATIONS OF THE RELAY ATTACK ON PKES SYSTEMS

As this messages sent over UHF it will reach the car even if the car is within a hundred meters 11. The car will therefore unlock. Once that the attacker has access to the car, the signals from within the car are relayed and the key will now believe it is inside the car and emit the *allow start* message. The car can now be started and driven. When the attacker drives away with the car, the relay will no longer be active. The car may detect the missing key; however, for safety reasons, the car will not stop, but continue running. Similarly, the car might detect a missing key for several other reasons including if the key battery is depleted. Some car models will not notify the user if the key is not found when the car is on course, while some will emit a warning beep. None of the evaluated cars stopped the engine if the key was not detected after the engine had been started. This attack therefore enables the attackers to gain access (open) and to get authorization to drive (start and drive) the car without the possession of appropriate credentials.



ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Figure (4) PKES system

The practical risks of such attacks are reported to be reduced as the attacker needs access to the ODB-II communication port, which requires being able to open the car. There lay attack we present here is therefore a stepping stone that would provide an attacker with an easy access to the ODB-II port without leaving any traces or suspicion of his actions. Moreover, as the car was opened with the original key if an event log is analyzed it would show that the car owner did open the car.

VII. COUNTERMEASURES

In this section we discuss countermeasures against relay attacks on PKES systems. We first describe immediate countermeasures that can be deployed by the car owners. These countermeasures largely reduce the risk of the relay attacks but also disable PKES systems. We then discuss possible mid-term solutions and certain prevention mechanisms suggested in the open literature. We finally outline new PKES system that prevents relay attacks. This system also preserves the user convenience for which PKESsystems were initially introduced.

7.1 Immediate Countermeasures

Shielding the Key One obvious countermeasure against relay attacks is to prevent the communication between the key and the car at all times except when the owner wants to unlock the car. The users of PKES-enabled cars can achieve this by placing the car key (fob) within a protective metallic shielding thus creating a Faraday cage around the key. As mall key case lined with aluminum might suffice for this purpose. While the key is in the key case, it would not receive any signals from the car (relayed or direct). When the user approaches the car, he could take the key out of the case and open and start the car using the PKES system. The users who would opt for this countermeasure would lose only little of the convenience of PKES. Similar countermeasures have been proposed to block the possibility of remote reading of RFID tags embedded in e-passports. However, an attacker might be able to increase the reading power sufficiently to mitigate the attenuation provided by the protective shield. We note that designing a good Faraday cage is challenging [36]. Still, this countermeasure would make the relay attack very difficult in practice.

Removing the Battery from the Key Another countermeasure against relay attacks is to disable the active wireless communication abilities of the key. This can be simply done by removing the battery that powers the radio from the key. As a consequence, the UHF radio of the key will be deactivated. The key will then be used in the “dead battery “mode, which is provided by the manufacturers to enable the

Users to open the car when the key battery is exhausted. In this case, the car cannot be opened remotely but only using a physical key (the backup physical key is typically hidden within the wireless key fob). Given that the cars that use PKES cannot be started using a physical key, in order to start the car in the “dead battery” mode, the user needs to place the key in the close proximity of some pre designated location in the car (e.g., the car Start button). The car then communicates with the key’s passive LF RFID tag using

Short-range communication. Typically, wireless communication with the LF RFID tags is in the order of centimeters, thus making the relay attack more difficult for the attacker; however, depending on the attacker capabilities relay from a further distance cannot be fully excluded. This defense disables the PKES for opening the car, but is still reasonably convenient for starting the car engine. With such a defense, the realization of a relay attack becomes very difficult in practice. A combination of the two countermeasures would provide the highest protection, but would also be the least convenient for the users. It would essentially reduce the usability of a PKES key to the one of the physical key.

7.2 Mid-term Countermeasures

While the previous countermeasures require only simple actions from the car owner, and without involvement of the manufacturer, they also significantly reduce the usability of the key system. Here, we present some lightweight modifications that provide better usability. Those modifications would require only simple software or hardware changes to the key system. While they are not solving the main cause of the problem, they do provide mitigation that are applicable immediately (by a software update or a key fob exchange or modification).Software Only Modification A simple software modification to the keyless vehicle unit could be provided to allow the user to temporally disable the PKES. When a user is closing the car by pushing the close button on the key fob the PKES would remain disabled. That is, the car would open (and allow start) only after the user pushes the open button on the key fob. This effectively allows the user to deactivate the PKES system by simply pushing the close button. This countermeasure would be used

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

for example by a car owner when parking in a unsafe place such as an underground parking or a public place. On the other hand if the car is closed by pushing the button on the door handle or simply by walking away from the car, the PKES system is used for closing the car and the car would therefore allow passive keyless entry and start.

7.3Access Control Restrictions

At least one car model enforced some more strict policy. For example, the car would quickly stop sending signals after the door handle was pulled out without detecting the presence of a key. While not preventing the relay attack it forces the attacker to be well prepared and to be synchronized, the door handle needs to be pulled out when the key holder passes in front of their laying antenna. In several cases, on this car model, the alarm was triggered and it was possible to disable it only by pushing the open button on the key fob. This is certainly deterrent to a thief. However, this again does not prevent the attack to besuccessful.Hardware Modification Adding a simple switch to the key would produce a similar countermeasure to that of removing the battery from the key fob. This switch would disconnect the internal battery allowing the user to temporarily disable the PKES functionality of the key, while keeping convenience of PKES. Variants of this modification would keep the possibility to use the active open (i.e. opening the car by pushing the button on the key fob) while deactivating only the passive entry.

VIII. CONCLUSION

In this paper, we have introduced and discussed security needs for wireless vehicle-to-infrastructure and vehicle-to-vehicle communication. We have adapted a well-known tax-anomy to the vehicle setting and discussed for each of five defense-in-depth layers the specific applicability and considerations of each layer. The main challenge ahead is the creation of lightweight defense mechanisms. We stress the importance of timely research and deployment of defensive mechanisms in all layers of defense.

REFERENCES

[1] *http://www.mercedes-benz.com/*.
[2] *http://en.wikipedia.org/wiki/Smart key*.
[3] *http://en.wikipedia.org/wiki/Keyless Go*.
[4] *http://vintrack.com/SIU.html*.
[5] Ettus research llc. http://www.ettus.com/.
[6] A. Alrabady and S. Mahmud. Some attacks against vehicles'passive entry security systems and their solutions. *Vehicular Technology, IEEE Transactions on*, 52(2):431 – 439, March 2003.
[7] A. Alrabady and S. Mahmud. Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs. *IEEE Transactions on Vehicular Technology*, 54(1):41–50, January 2005.
[8] S. C. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubin,and M. Szydlo. Security analysis of a cryptographicallyenabledRFID device. In *Proc. of the 14th USENIX Security Symposium*, Berkeley, USA, 2005. USENIX Association.
[9] S. Brands and D. Chaum. Distance-bounding protocols. In *EUROCRYPT '93*, pages 344–359, Secaucus, NJ, USA,1994. Springer-Verlag New York, Inc.
[10] S. Capkun, L. Butty´an, and J.-P. Hubaux. SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. In *Proc. of the ACM Workshop on Security of AdHoc and Sensor Networks (SASN)*,Washington, USA, October 2003.
[11] S. Capkun and J.-P. Hubaux. Secure positioning in wireless networks. *Selected Areas in Communications, IEEE Journal on*, 24(2):221–232, February 2006.
[12] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore. So
near and yet so far: Distance-bounding attacks in wirelessnetworks. In *Proceedings of the European Workshop on Security and Privacy in Ad-hoc and Sensor Networks (ESAS)*,2006.
[13] N. T. Courtois, G. V. Bard, and D. Wagner. Algebraic and slide attacks on KeeLoq. In *Fast Software Encryption: 15thInternational Workshop, FSE 2008, Lausanne, Switzerland, February 10-13, 2008, Revised Selected Papers*, pages 97–115, Berlin, Heidelberg, 2008. Springer-Verlag.
[14] B. Danev, H. Luecken, S. Capkun, and K. Defrawy. Attackson physical-layer identification. In *Proc. of the 3th ACMConference on Wireless Network Security (WiSec)*, pages89–98. ACM, 2010.
[15] Datagram. Lock picking forensics. Black Hat USA Briefings, 2009.
[16] Y. Desmedt, C. Goutier, and S. Bengio. Special uses and
abuses of the Fiat-Shamir passport protocol. In *CRYPTO*,
pages 21–39, 1987.
[17] Anbuselvi S., Rebecca J., "A comparative study on the biodegradation of coir waste by three different species of Marine cyanobacteria", Journal of Applied Sciences Research, ISSN : 1815-932x, 5(12) (2009) pp.2369-2374.
[18] P. Dodd. *The low frequency experimenter's handbook*. Herts: Radio Society of Great Britain, 2000. ISBN : 1-872309-
65-8.
[19] Bharatwaj R.S., Vijaya K., Rajaram P., "A descriptive study of knowledge, attitude and practice with regard to voluntary blood donation among medical undergraduate students in Pondicherry, India", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 6(S4) (2012) pp.602-604.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

[20] S. Drimer and S. J. Murdoch. Keep your enemies close: distance bounding against smartcard relay attacks. In *Proceedingsof 16th USENIX Security Symposium*, Berkeley, CA,USA, 2007. USENIXAssociation.
[21] Raj M.S., Saravanan T., Srinivasan V., "A modified direct torque control of induction motor using space vector modulation technique", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 20(11) (2014) pp.1572-1574
[22] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux,and J.-Y. Le Boudec. Effectiveness of Distance-DecreasingAttacks Against Impulse Radio Ranging. In *3rd ACM Conferenceon Wireless Network Security (WiSec)*, 2010.
[23] Rajasulochana P., Krishnamoorthy P., Dhamotharan R., "An Investigation on the evaluation of heavy metals in Kappaphycus alvarezii", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384, 4(6) (2012) pp. 3224-3228.
[24] F.-L. W. Frank Stajano and B. Christianson. Multichannel
protocols to prevent relay attacks. In *Financial Cryptography*,
2010.
[25] Jasmine M.I.F., Yezdani A.A., Tajir F., Venu R.M., "Analysis of stress in bone and microimplants during en-masse retraction of maxillary and mandibular anterior teeth with different insertion angulations: A 3-dimensional finite element analysis study", American Journal of Orthodontics and Dentofacial Orthopedics, ISSN : 0889-5406, 141(1) (2012) pp. 71-80.
[26] S. Gezici, Z. Tian, G. Giannakis, H. Kobayashi, A. Molisch,H. Poor, and Z. Sahinoglu. Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks. *Signal Processing Magazine, IEEE*, 22(4):70–84,July 2005.
[22] G. Hancke. Practical attacks on proximity identification systems (short paper). In *Proc. of the 27th IEEE Symposium onSecurity and Privacy*, 2006.
[23] G. P. Hancke and M. G. Kuhn. An RFID distance bounding protocol. In *SecureComm '05: Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pages 67–73, Washington, DC, USA, 2005. IEEE Computer Society.
[24] G. P. Hancke, K. Mayes, and K. Markantonakis. Confidence in smart token proximity: Relay attacks revisited. *Computers& Security*, 28(7):615–627, 2009.
[25] Y.-C. Hu, A. Perrig, and D. B. Johnson. Wormhole attacks in wireless networks. *IEEE Journal on Selected Areas in Communications*, 24(2):370–380, 2006.
[26] B Karthik, TVUK Kumar, EMI Developed Test Methodologies for Short Duration Noises, Indian Journal of Science and Technology 6 (5S), PP 4615-4619, 2013.
[27] S.Rajeswari, Blurred Image Recognition by Legendre Moment Invariants, International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN 2278 – 8875,pp 83-86, Vol. 1, Issue 2, August 2012
[28] G.Tamizharasi, S.Kathiresan, K.S.Sreenivasan, Energy Forecasting using Artificial Neural Networks , International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,ISSN: 2249-2615,pp 7-13, Volume2 issue-6 No1 Nov 2012
[29] K. Subbulakshmi,An Embedded Based Web Server Using
ARM 9 with SMS Alert System,International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, ISSN (Print) : 2320 – 3765, pp 6485-6490,Vol. 2, Issue 12, December 2013.
[30] K. Subbulakshmi,VLSI Implementation of Evolvable PID
Controller,International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,ISSN (Print) : 2320 – 3765 , pp 6572-6579,Vol. 3, Issue 1, January 2014.
[31] K.Subbulakshmi,Three Phase Three Level Unidirectional PWM Rectifier,International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering,ISSN (Print) : 2320 – 3765, pp 7090-7096, Vol. 3, Issue 2, Febuary 2014.