The Eighth International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, Serbia

ROAD VEHICLE EMBEDDED IOT SECURITY

LYUDMILA ZHAROVA
New York Institute of Technology, New York, NY, USA, lzharova@nyit.edu

VITO LEGGIO
Faculty of Organizational Sciences, UB, Belgrade, Serbia,leggio505315d@fon.bg.ac.rs

ALEKSANDAR MIHAJLOVIĆ
School of Electrical Engineering, UB, Belgrade, Serbia, aleksandar.mihajlovic@etf.rs

SHAWN CAMPBELL
IT Systems, New York, USA, shawnm.campbell@gmail.com

RADOMIR A. MIHAJLOVIĆ
New York Institute of Technology, New York, USA, rmihajlo@nyit.edu

Abstract: *Users of motorized vehicles are continuously demanding new improvements that would further increase the efficiency,safety, and user friendliness, i.e., simplicity and pleasure of operating such vehicles. Computing and communication technologies have been major contributors driving and justifying these trends. Faced with the phenomena of the massive proliferation of computing micro systems as embedded components on board of modern motorized vehicles, we are forced to acknowledge the issue of security and reliability of such micro systems' operation. We present here a brief historical overview of the automobile embedded computing development, we analyze the complexity of automobile computing, it's I/O exposure to benign as well as malicious user interaction, the standardization of automobile computing networks and problems related to opening these networks to the Internet, i.e., the problems of internetworking these networks. In addition we present a unique model of the malicious attack surface that motorized vehicles may present on various levels of abstraction hierarchy.*

Keywords: *Internet of Things (IoT), Security,In-Vehicle Networking (IVN), Privacy, V2V, Stuxnet.*

1. INTRODUCTION

After several shocking road accidents, such as the tragic car crash in Paris (August 30, 1997) that claimed the lives of British Princess Diana and her friend Dodi Fayed [1] and the accident in California (June 18, 2013) where investigative journalist Michael Hastings died [2], the authors of this paper and several of their coworkers have decided to devote more attention to the problems of road vehicle electronic security and the dangers of so called "Car Hacking."This topic has attracted several groups of researchers and cyber security specialists [3-6], as well as all of the car manufacturers worldwide. The importance of the topic is self evident.

To be specific and to avoid dealing with all possible vehicles, (flying, floating and terrestrial vehicles), in our discussions we focus on the modern road vehicles, which are interchangeably referred to as land vehicles, motorized road vehicles, automobiles, autos or cars. Although inspired by unusual car accidents, we group cars, trucks and recreational vehicles (RVs) under one umbrella class of vehicles that we call road vehicles.

It is well known that modern automobiles contain a significant number of electronic devices whose sole purpose is diverse measurement signal collection, control signal generation and signal transmission. Digital electronic devices found on board of road vehicles capable of performing various computation and communication activities are known as Electronic Control Units or ECUs [3]. To simplify our discussion, we assume that data input or sensor devices may also be included in the class of ECUs. Common modern automobile contains almost one hundred ECU devices, each dedicated to some electrical signal processing activity associated with a physical vehicle part that we may refer to as a vehicle Thing (vT). Each ECU presents an associated vT as a digital device. The ECU transforms the analog and possibly the non-electronic vT into a digital device that can compute and may be networked with other ECUs. For example, there is an ECU that "monitors" hand break or "opened door state" sensor. Some more sophisticated ECUs may be in charge of detecting ignition key presence and that the passenger is not in the car, producing a joint status signal that "instructs" another ECU in charge of preventing the car door lock from operating. Acar that would prevent a user from locking doors and exiting the car with the keys in the ignition, would appear as an intelligent or smart car.

Figure 1 illustrates an example of the ECU attached to some vTs embedded in the physical road vehicle system labeled as the "Monitored & Controlled Plant." Evidently,

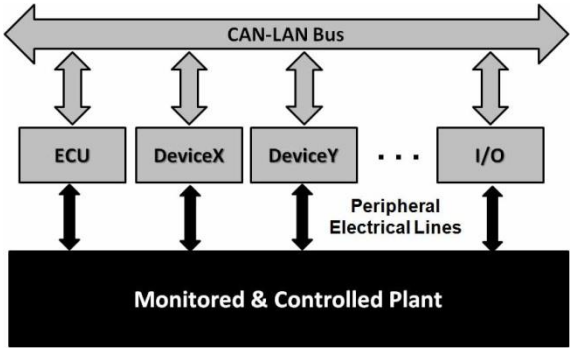

Figure 1: CAN-LAN bus topology minimizes wiring complexity of fully connected LAN and simplifies individual device and ECU activity synchronization.

once purely mechanical road vehicles have grown into mostly electrical and electronic devices. It may even be appropriate to look at the modern road vehicles as a network of computer hosts on wheels with network nodes loaded with millions of lines of code.

Our approach to IoT systems (illustrated in Figure 1) with clear division of "Things" related plant and "Internet" related network technology represents original way of extending security of complex systems such as nuclear power plants or electric grids to IoT systems found on board of road vehicles or vehicles of any kind.

ECU networks may be designed as single trunk or bridged local area networks that are commonly referred to in the literature as In-Vehicle Networks or IVNs. IVNs are as inevitable elements of today's automobile as Local Area Networks (LANs) may be unavoidable in modern business offices. From the high-end to the lower classes of automobiles, IVNs are being expanded and rapidly developed aiming atthe increased vehicle intelligence that may eventually lead to fully autonomous or driverless road vehicles. Smart or intelligent vehicles with complexcomputing architectures and underlined software present a wide spectrum of possible security holes, i.e., attack vectors that can be exploited in malicious attacks.

There are various architectures and implementations of the IVN in use today. We are still far from a unified standardized architecture accepted by all motorized vehicle manufacturers. Each of these networks operate under different specifications and provide different data transmission speeds (i.e., offers different transmission line bandwidths). As a result of this diversification, the application of IVNs may vary based on the data transmission speed requirements of the various vehicle components that they support. The most common networks that we may find in today's vehicles are:

- Controller Area Network (CAN)
- Local Interconnect Network (LIN)
- FlexRay
- Media Oriented Systems Transport (MOST)

CAN IVNs are used for basic device to device control, status and data message transmission, i.e., to facilitate medium speed link implementations, LIN IVNs are used for low-cost body electronics and lowest data-rate functions, FlexRay networks are convenient for safety critical tasks such as steering wheel and brake control message exchange, and MOST networks are high speed networks used for automobile infotainment systems.

Each of the mentioned approaches to IVN implementation may have certain desirable features, but among all of them CAN dominates and may be found in almost every modern road vehicle. Due to the limited scope of this paper we shall briefly present only details of CAN and will leave discussion about the other types of IVNs for our future presentation.

2. CAN IVN PROTOCOL

Controller area network is a serial bus based local area network with L1 strict physical layer specifications [7] and strict L2 data link (DL) protocol specification [8][9] where L1 and L2 are the bottom two layers of the seven ISO-OSI model [10]. The CAN bus with signaling speeds of up to 1Mbps is used to establish links between ECUs or links between vehicle's onboard computer with the sensors that monitor various vT's. Figure 2 illustrates CAN bus node basic structure.

The CAN protocol was developed in the mid 1980's at Bosch for in-vehicle sensor networking. CAN has represented an important development step aimed at the reduction of the overall complexity and cost of the automobile electronic system. Prior to the CAN, if a new feature had to be added to an automobile, it meant adding additional wiring to the overall mash of wires to connect up the new feature device in a point to point fully connected network topology. By using a serial bus, the need for point to point full connectivity cabling became unnecessary. Each device had to be simply attached to the CAN bus as a node utilizing standardized bus interface (See Figures 1 and 2).

The CAN bus lines are made of two parallel twisted pair lines that are used in biased differential mode to backup each other and ensure data transmission in the event of one line failure [9]. Two wire-lines transmit opposite versions of the biased binary data pulse signal with one line called CANH high and the other CANL low line. The lines act as two lines of the differential signal transmission historically used for analog telephone voice signal transmission. When the CAN bus is in idle mode, both lines present bias voltage of 2.5V which makes line-to-line difference of 0V. Any noise signal of the same level present on both lines produces 0V differential value which makes CAN bus Electro-Magnetic Interference (EMI) noise immune. When high data bit is being transmitted, the CANH goes to +3.75V and the CANL goes low to +1.25V, producing line to line signal level difference of 2.5V. For low data bit values signal levels are opposite [7].

Differential nature of the CAN bus signaling, low signaling rates of under 1Mbps, and relatively short line length of less than 40m [8], makes the bus fairly robust.

In the electrically noisy environment under the hood of the road vehicles, this feature of the CAN bus makes it difficult to jam, i.e., perform an attack in the physical L1 layer.

Each node on the bus is connected to both lines and can use the bus rate in a half duplex mode, i.e., may send or receive data but not send and receive simultaneously. The nature of the CAN bus line set and signal format is important to an attacker that plans physical layer jamming attack.

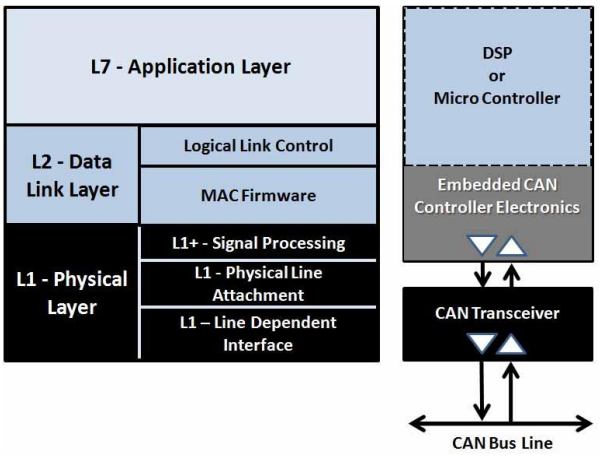

Figure 2: Simplified ISO-OSI relevant CAN bus node layered model.

In the seven layer ISO-OSI [10] or four layer Internet architecture model [11][12], the lower end of the L2 Data Link (DL) layer is defined as Media Access Control (MAC) protocol. CAN MAC layer is specified to operate like Ethernet Carrier Sense Multiple Access/Collision Detection (CSMA/CD) protocol. When the bus is idle (Carrier is not sensed), any node may start to transmit its data frame by sending start of frame (SOF) bit. If several nodes start transmitting their frames at the same time (Collision is detected) an arbitration process is started to control which node may transmit while the other nodes have to back off and delay their transmission (Perform multiple access). The bus arbitration process used in CAN protocol is CSMA/CD with Arbitration on Message Priority (AMP). The CAN bus MAC protocol is known as CSMA/CD+AMP.

Each message data frame on the CAN bus has a unique ID that determines the identity of the sending node and the priority of the message. Priority based arbitration is used when two IVN nodes attempt to use the bus media at the same time. The message with the lower priority numerical value as higher priority message wins and the lower priority message is retransmitted on the next bus cycle. Priority based protocol of arbitration guarantees that critical ECU will get their messages in its real time. One of the attack exploits may target the priority arbitration protocol and delay the delivery of critical messages.

CAN IVN broadcast nature has all messages that appear on the bus delivered to all IVN nodes. Individual nodes are filtering all non-relevant messages and are accepting only relevant data which are passed up the stack for processing in the application layer (See Figure 2). Apparently, CAN bus as a CAN-LAN core resource and central point of failure is possible to attack and overload via physically planted malicious bus node device or ECU. Such a node device is easy to build [13][14]. In a L1/L2 Denial of Service (DoS) attack, remotely controlled malicious node may jam the bus with a flood of high priority rogue messages and prevent other vital operational messages from being transmitted. Defensive mechanisms that can be used to prevent physical addition of malicious CAN nodes are open for further research and development (R&D) work.

The CAN protocol is completely implemented on board of the CAN controller. The protocol for data link control is standardized by the ISO 11898-1 [15] document while the Medium Access Unit (MAU) i.e., electrical line interface level of the CAN node is specified by the ISO 11898-2/3 documents [16][17].

3. CONNECTING VEHICLE TO THE OUTSIDE WORLD

Modern automobiles are delivered with a number of data collecting sensors that may be classified into two major groups:

- Vital engine monitoring sensors, and
- Vehicle monitoring sensors of direct user interest.

The second class of sensors would cover: Global Positioning System (GPS) vehicle location sensor, temperature, speed, braking system sensors such as the slippery road detection sub system, etc.

Most of the sensors and the format of data that these sensors report are designed in a proprietary manner, to which we refer to as Original Equipment Manufacturer (OEM) design. Some of the data formats and datadelivery technologies are already standardized or are in the process of standardization. An example of a standardized service and data format is the GPS data delivery and presentation vehicle user service.

On the higher levels, data are presented via:

- User interface (UI) programs and devices,
- Application communication protocols, or
- API class or function library.

For instance delivered music, video, Web browsing, road maps and traffic congestion reports data are presented via high level user services which has to be differentiated from the application program service such as Web or DNS service. Numerous user services have found their way into the vehicle by means of the IVN via Internet and IVN access points. The presence of such services and the need to have wireless Internet access point devices as IVN nodes has introduced additional level of systems

complexity that has to be defended from malicious attacks.

4. VEHICLE TO VEHICLE LINK SECURITY

A vehicle-to-vehicle (V2V) communication protocol and vehicle subsystems used for cooperative collision anticipation and warning as well as V2V ad-hoc networking are being introduced during the last decade [18][19][20]. V2V ad-hoc networking as well as vehicle-to-roadside (V2R) communications require establishment of wireless links and appropriate IVN access point node. Although promising to dramatically reduce road accidents via active safety mechanisms and promising to enable several new user level services, the opening of the IVN to wireless access over yet another link introduces a whole new attack vector and potential exploits.

The IEEE 802.11p is an extension of the IEEE 802.11 standard and was introduced to add wireless (WiFi) access in the band of 5.9GHz to IVN and specify links of short data frames needed for Intelligent Transportation Systems (ITS) sort of applications. Using the IEEE 802.11p IVN compliant access point, vehicles are able to establish temporary links with nearby vehicles or roadside V2V supporting systems. Due to the short time to live (TTL) nature of V2V and V2R links and dynamically changing link end points, no authentication protocol is proposed by this standard. A V2V link is established between two vehicles as soon as they are in range of each other. A warning may be issued to a vehicle user if a vehicle that may not be visible suddenly take some threatening action.

This feature, while presenting great possibilities as it relates to safety, will also present challenges from a security standpoint. If we allow communication without authentication we may not be able to trust the data that is being delivered. Some of the possible solutions that could minimize problems caused by the missing authentication protocol could be as follows:

1) Use application layer firewall that could filter data that are received via 802.11p standard link.
2) Restrict physical actions caused by the data received via V2V link. For instance, actions could be audiovisual vehicle user warning and not command message sent to some important ECU and vT causing vehicle maneuver action on the user's behalf
3) Restrict V2V message delivery only to a specific IVN segment that does not cover any critical ECU set.

These solutions could be applied to other V2V protocols that may be different from the 802.11p, (e.g., custom Bluetooth, Wi-Fi or cellular link).

With the distance limitation to roughly 10m, Bluetooth protocol may be inconvenient for use in the attack exploits on the road. It is very hard to maintain short distance between the attacker and target vehicle in motion. However, an attack could be pre launched at a target vehicle while being stationary by delivering malicious data payload that may be executed at some later point in time.

WiFi links provide greater opportunity to execute an attack than Bluetooth links.

Cellular telephony links have been proven to be vulnerable to attacks and should be voided in all V2V network based applications.

The concept of vehicle to vehicle (V2V) communications with vehicles being linked directly with neighboring vehicles or indirectly via road side units assumes individual IVN exposure with all IVN ECUs attached to the potential malicious data traffic. Lotfi Ben Othmane at al.[20] has developed an estimations of the likelihoods of several security sorts of attacks aimed at V2V networked vehicles. Most of the analyzed vehicle attack exploits were found to be very unlikely. The survey showed that attacks on connected vehicles must be rapid, before being discovered or before the attack context would change, and be designed and executed by very sophisticated attackers with profound knowledge about the target.

5. V2V PRIVACY ISSUES

Vehicle to Vehicle (V2V) applications employ basic safety message (BSM) exchange between vehicles providing each other with additional safety data not delivered by the on board sensor networks. In order to minimize response time, by default design, BSM data is not encrypted. In order to provide data protection, BSM data packets are secured with a digital certificate which guarantees message authenticity, [21,22,23].

Since every digital certificate contains the owner's identification data [24] illegal or unplanned access of the vehicle digital certificate may lead to the illegal private data exposure, i.e., invasion of privacy. The main privacy concerns can be summarized as:

- Vehicle owner tracking – A study performed in 2009 by PARC indicates that more than 5 percent of US citizens can be identified by the pair of data identifying their place of work and their residence address. Tracking unique vehicle digital certificate enables reliable determination of both of these dataitems. Apparently V2V technology enables tracking vehicle geographical location [25] which onetime may be desirable and another time may not be.
- In traffic vehicle behavior tracking and automatic traffic violation citation distribution. Digital certificate could reinforce existing network of intersection monitoring CCTV camera networks and enable automated issuance of traffic violation citations. Such a facility would greatly increase local government revenue and as a deterrent improve traffic safety while outraging community of drivers.

It is reasonable to expect that the vehicle owners community aware of being continuously tracked, would massively protest and possibly endanger the acceptance of

the useful and secure V2V technology based on the digital certificate. To avoid such a situation unique, global and permanent vehicle identification has to be abandoned and possibly replaced with the locally unique vehicle identification with the limited time to live (TTL) identification data record (also known as Personally Identifiable Information or PII).

Some of the privacy protection methods may involve the following:

- Preventing PII message wireless transmission Data such as vehicle owner's name, id number, vehicle license plate, vehicle identification number (VIN) or similar should not be a part of any wireless link data frame.
- Unique digital certificate should identify logical user, Logical user entity relevant to the user's pass-code and not the user, i.e., user's private identity data should be used in the digital certificates. Anonymous certificates where CA is not provided with the complete user's data
- Rotating digital certificate that dynamically is changing, e.g., user uses N certificates each week, rotating them so one certificate can't be used to track a person or vehicle, protecting against the home/work pairings found in the PARC study.

Necessary steps must be taken to preserve privacy of the vehicle owner while maintaining secure wireless V2V communication.

6. STRUCTURED APPROACH TO VEHICLE SECURITY

Some of the IVN networked ECUs are in charge of communications with the outside world as well as the internal ECUs. ECUs that are exposed to outside network access pose the biggest security risk to the vehicle and car users. Such ECUs permit internal IVN access that must be well controlled. The spectrum of exploits available to potential IVN intruder is determined by the additional layer of access control options in charge of individual ECU access.

We propose a multilayered model of vehicle security maintenance based on the extension of the network perimeter concept.

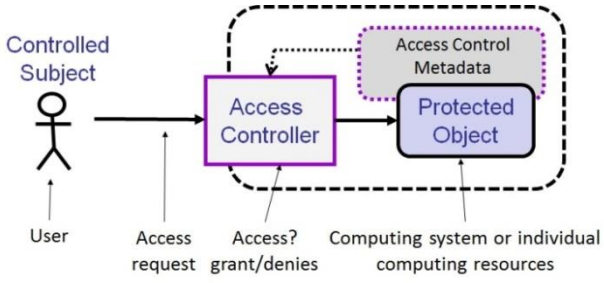

Figure 3: Elementary access control model.

Our multilayer security control model is based on the multiple levels of access control mechanisms that start with the outmost control point represented by the physical car entry mechanism that may be direct key contact or wireless contactless based. We refer to this outmost access control as control AC_0. Figures 3 and 4 illustrate the layout of access control points where the point AC_1 represents the vehicle ignition key. There are numerous personalized mechanisms that may be employed to implement AC_0. From the ignition point on, at the lowerlayers of the access control hierarchy we find electronic devices communicating according to certain protocol specification.

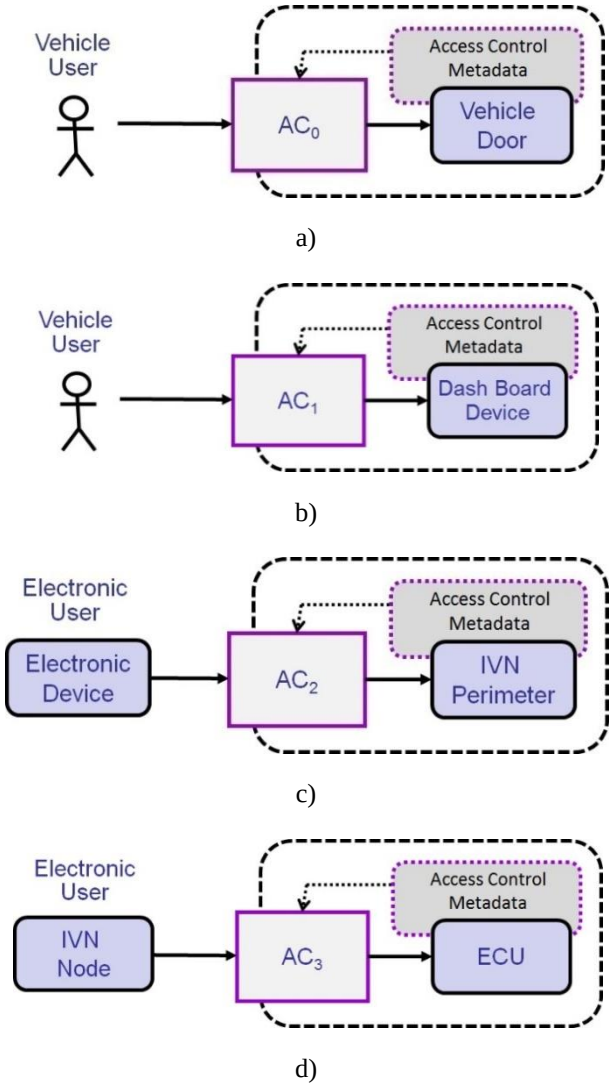

Figure 4: Multi level access control providing defense in depth layered protection of IVN ECUs.

7. REMOTE ATTACK PATTERN

By the classification of attacks (See [24]) on some protected resource, successful attack may result in:

- The denial of resource service (DoS) to legitimate resource users, or
- Illegal resource access and use.

The DoS attack may be:

- Hard DoS, with total destruction of the resource, or

- Soft DoS, resulting in reduced quality of resource service (QoS).

Both sorts of DoS attacks on the vehicle in motion may be catastrophic for the vehicle user and other vehicles that may be consequentially involved. In one of the attack patterns secondary target vehicle acting as a zombie or proxy attacker vehicle, may be subjected to electronic hard DoS while performing physical hard DoS on the primary target vehicle. This sort of the two stage attackis possible with very sophisticated vehicles with optional V2V primary to secondary target communications.

We distinguish two general sorts of the vehicle attacks:

- Physical, and
- Electronic or cyber attack.

A simple example of a hard DoS physical attack is the case of a planted car bomb or the use of an improvised explosive device (IED) placed alongside the road. IED hard DoS attack presents the greatest threat to US troops deployed overseas. An example of the soft physical DoS attack would be contamination of the gasoline or other vehicle liquids and sabotage on various vehicle physical parts, i.e., vTs. Common vT attacks involve vandalizing a vehicle, e.g., bycutting pneumatic hose or severing internal wire lines. In case of soft DoS attack, vehicle remains operational with suboptimal performance characteristics that may lead to total denial of vehicle service. Partial model of the vTs found in a common vehicle is shown in Figure 5. Our detailed model of the road vehicle is beyond the scope of this presentation and is not given here.

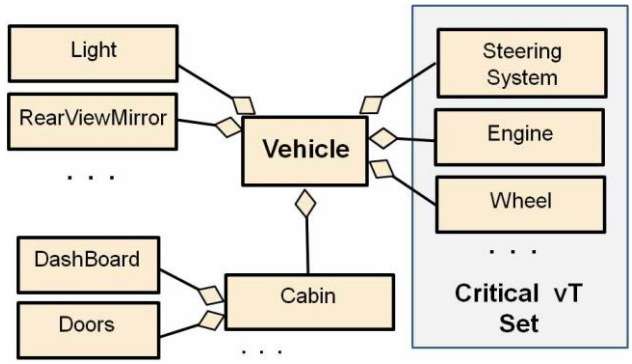

Figure 5: Partial UML class diagram of a vT set found in the common road vehicle.

Figure 5 shows distinguished set of critical vTs. Hard DoS on critical vTs may be tragic for the vehicle user. When an attacker desires to physically harm vehicle user, attack pattern has to involve critical vT set elements as favored targets.

As a rule, malicious cyber-attacks of remote modern automobile goes through following stages:

- Attacker establishes attack stepping stone device or IVN access point (AP).
- Using the IVN AP attacker gains access to the IVN of a vehicle.
- Attacker injects exploit message set into the IVN traffic stream.
- Injected message data controls targeted ECU and the vT behind it.

Primary subject of our work are problems of vehicle cyber attack of both, DoS and illegal access kinds via wireless link, i.e., remote cyber attacks.

We classify attacks on any protected system (System employing access controls) as:

- Front door, and
- Backdoor attacks.

Implementation of the protection of modern road vehicles is primarily focused on the access control at various user interface points in the vehicle cabin, (See Figure 6). The set of these user interface points forms physical front door of the system. Vehicle manufacturers offer variety of physical implementations of the physical front door access controls and penetration testers and hackers diligently work discovering new front door attack exploits.

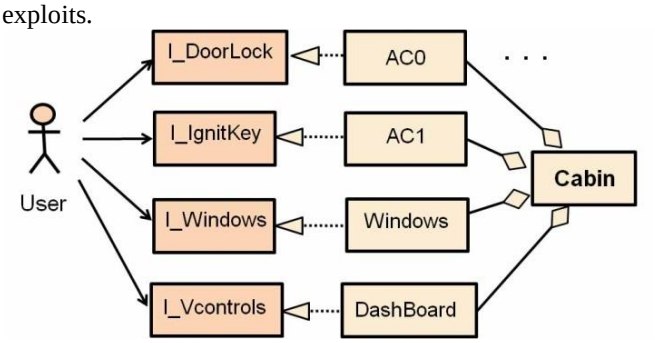

Figure 6: Partial UML class diagram of the vehicle cabin elements and implemented user interfaces.

Installing an IVN AP device in the initial phase of the DoS attack, may involve preliminary front door or backdoor attack. Physical backdoor vehicle attacker avoids standard user interface points and may be performed in repair shops, parking garages, in the streets, etc. Planting IVN AP (later to be used in the wireless cyber-attack), is equivalent to the initial steps taken with the 2010 first digital weapon use, known as the Stuxnet. We treat the Stuxnet and DoS road vehicle cyber-attack as two isomorphic attacks. In our models, a set of road vehicle things or a set of nuclear power plant things are equally treated as monitored and controlled plant (See Figure 1).

At the lowest level (physical level), electronic or cyber attack involves illegal use of ECU registers associated with some of the critical vTs. IVN ECUs appear precisely as I/O controllers attached to the computing host systems I/O bus. As specified in [24] all programmable I/O controllers, and consequently ECUs contain three sorts of registers:

- Read only status registers,
- Write only command or instruction registers, and
- Read/Write data registers.

Assuming control of the targeted IVN ECU implies use of all three sorts of registers with particular focus on the ECU command registers. Denying access to that type of ECU registers to the unauthorized command message is ideal IVN protection mechanism. Unfortunately most of the modern IVN and ECN solutions do not implement ECN instruction register access control which is in its simplest possible form implemented in the modern Central Processing Units (CPUs). Namely, the execution of the privileged CPU instruction must be accompanied by the appropriate privilege level flags or privilege ring code maintained in the Program Status Word (PSW) CPU register set [26]. Following this line of design reasoning, we propose that as the last perimeter of defense in depth IVN architecture, we have access control of each ECU command. In his thesis [27], Rogers describe methods of possible circumventing privilege level control of certain CPU instructions. The work of Rogers proves that the incomplete protection is not possible in the simple binary session between the actor and the protected resource. The last two authors have explicitly defined the fundamental condition for secure session implementation [24] which clearly states in an axiomatic form that binary session cannot be made secure without a third session node. In other words the only ternary session may recursively guarantees security of the production binary session. To be specific, secure binary production session employs two security related meta-sessions involving production session nodes and third secure domain management node. In our future paper we propose a solution of secure access control of command messages at the IVN ECU instruction registers.

8. DEFENDING ROAD VEHICLE IOT

A network on board of road vehicles connects a set of vTs via ECUs acting as interface. The combined set of the vT and the associated ECU form computing thing that can be networked, a thing that constitutes anode on the vehicle based Internet of Things (IoT). Vehicle based IoT is one specific example of the IoT that significantly differs from the commonly found IoT. Fundamental difference in question is that:

- Vehicle IoT devices have solid power source,
- The lines interconnecting IoTs are not wireless but wire line based,
- Justified by the absence of the fragile power sources and availability of funds to invest improving high price ticket item such as a road vehicle, computing power (CPU and memory) capacity does not have to be minimized.
- IoT wire lines are robust and reliable
- Data transmission rates do not have to be minimized

Taking all of the above mentioned features, we may conclude that implementing security extensions of the vehicle IoT on any level of complexity should not be limited by the commonly found constraints in typical IoT networks such as wireless sensor networks.

Practically every American carmaker now offers IVNs capable of communicating with the external world via wireless links using a cellular service, Wi-Fi links (e.g., General Motors' OnStar, Toyota's Safety Connect or Ford's SYNC). All of the carmakers are actively engaged in the research and development of secure wireless vehicle IVN access solutions. Their engineers test their vehicles against wireless attacks. However, we must stress that the pace of mechanical vehicle engineering and computing technology evolution are significantly disproportionate. From the new vehicle design studio to the dealership sales floor, new model development and manufacturing may take on average up to four years [28]. At the same time new designs of sophisticated computerized cell telephones development with massive amount of new software features may be launched in less than a year. With such a vehicle mechanics to IVN computation development asymmetry, a car may be way behind the new digital developments that may include new, let us say zero day, malicious software tools and hacker's exploits. Apparently, motorized vehicles must be open to timely, i.e., frequent software patching, where frequent software patching opens new avenues of creative "car-hacking".

In order to engage as large as possible number of talented hardware and software specialists, we take a strong position that all road vehicle attacks must be urgently reported and widely advertised, i.e., must be open. Further research and development on the topic of secure timely vehicle network hardening is more than necessary.

ECUs are located in various places throughout the car. ECUs controls almost every aspect of the modern automobile, they take input from sensors and provide output to actuators. ECUs are executing proprietary code on proprietary hardware micro architectures and as such are very hard to infect. Even though most of the ECUs are running firmware code that is hard to erase and replace by some viral code, a dedicated attacker will devote time to backward engineer sample devices preload infected firmware and physically replace the ECU on the IVN with the malicious version. Physically guarding road vehicle from the unauthorized physical access is essential in the overall security measure set. Malicious ECU, shown in Figure 3 c) and d) may be used to perform illegal accessto other ECUs on the IVN or to execute DoS sort of an attack on any element of the IVN including the IVN bus.

9. CONCLUDING REMARKS

Several cases of strange accidents that have resulted in the deaths of prominent public and media figures have inspired a series of conspiracy theories claiming that modern high end vehicles such as Mercedes-Benz automobiles (e.g., 280-S [1] or C250 coupe [2]) may be maliciously attacked using cyberspace technologies. One of the most shocking Mercedes-Benz vehicle accidents has caused Russian President Putin's driver death [29]. In this tragic accident, Mercedes-Benz vehicle made a

similar maneuver to the one described in [1], crashed into a highway fence, crossed the fence and collided heads on with President Putin's official BMW vehicle moving in the opposite direction. Conspiracy theorists could classify the last accident as the first case of hacking cars to be used as a guided weapon. Unusual sequence of deadly car accidents involving the most sophisticated vehicles such as those manufactured by the Mercedes-Benz, definitely justify extraordinary attention to the road vehicle security and avoidance of possibly exploiting V2V communication between the physically attacking and attacked vehicles.

Since most of the original manufacturer's ECU software defects are timely patched we focus not on the defense against zero day attacks based on legitimate software bugs, but on the spear attacks based on the planted illegal IVN AP. Upon systems analysis of the vehicle elements, our explicit proposal how to defend against cyber attacks even after successful IVN AP installation (Initial step in the Stuxnet [30] or vehicle DoS cyber attacks), is to implement register level access control (See Figure 4 d). Since the standardization of the internal ECU implementations is still in its relative infancy, any modification of the existing ECU design or introduction of the new line of controllers is feasible and financially justifiable. Following the strategic recommendations of defense in depth, in addition to the register level security measures we could work on solutions which would prevent illegal IVN AP installation, i.e., detection of IVN nodes that are not originally built in the factory.

The scope of this text is practically limited. Under the given constraints, our presentation is focused on the most important elements of the topics of protecting road vehicles from cyber attacks. We leave additional details describing our work on structured approach to the security of the IoT networks embedded on board of motor vehicles for our future presentations.

REFERENCE

[1] "Princess Diana cover-up," The UK & Ireland Database, 2016.

[2] Mike Hogan, "Was Michael Hastings' Car Hacked? Richard Clarke Says It's Possible," The Huffington Post, Jun 26, 2013

[3] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., Savage, S., "Experimental security analysis of a modern automobile," In Proceedings of the 2010 IEEE Symposium on Security and Privacy, pp. 447-462.

[4] Pierre Kleberger, Tomas Olovsson, ErlandJonsson, "Security Aspects of the In-Vehicle Network in the Connected Car," 2011 IEEE Intelligent Vehicles Symposium (IV) Baden-Baden, Germany, June 5-9, 2011.

[5] Stephen Checkoway, Damon McCoy, Brian Kantor, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno,, "Comprehensive experimental analyses of automotive attack surfaces," SEC'11 Proceedings of the 20th USENIX conference on Security, 2011, pp.6-6.

[6] Mark Anderson, "Black Hat 2014: Hacking the Smart Car," Mark Anderson, IEEE Spectrum,

Aug 6, 2014.

[7] Steve Corrigan, "Controller Area Network Physical Layer Requirements," Texas Instruments Application Report, SLLA270–January 2008.

[8] M. Di Natale, "Understanding and using the Controller Area Network," October 30, 2008.

[9] Blackmore, J., & Monroe, S., "Overview of 3.3V CAN (controller area network) transceivers," Application Report, Texas Instruments. 2013.

[10] William Stallings, "Handbook of Computer Communications Standards: Open Systems Interconnection Model v. 1," The Macmillan database/data communications series, Macmillan, March 1988.

[11] Kevin R. Fall and W. Richard Stevens, "TCP/IP Illustrated, Volume 1: The Protocols," 2nd Ed., Addison-Wesley Professional Computing Series, Nov. 25, 2011.

[12] Douglas E. Comer, "Internetworking with TCP/IP Volume One," 6th Ed., Pearson, May 5, 2013.

[13] "CAN FD v1.0 LogiCORE IP Product Guide," Vivado Design Suite, PG223 November 18, 2015.

[14] Pat Richards, "A CAN Physical Layer Description," Microchip Technology Inc., AN228 note, 2002.

[15] "Road vehicles -- Controller area network (CAN) -- Part 1: Data link layer and physical signaling," ISO 11898-1:2015.

[16] "Road vehicles -- Controller area network (CAN) -- Part 2: High-speed medium access unit," ISO 11898-2:2003.

[17] "Road vehicles -- Controller area network (CAN) -- Part 3: Low-speed, fault-tolerant, medium-dependent interface," ISO 11898-3:2006.

[18] Hong Bong Kim, M. Emmelmann, B. Rathke, A.Wolisz, "A Radio over Fiber Network Architecture for Road Vehicle Communication Systems," Proc. IEEE Vehicular Technology Conf., VTC Spring 2005.

[19] Xue Yang, et al., "A Vehicle-to-Vehicle Communication Protocol for Cooperative Collision Warning," The Fifth IEEE International Conference on Networking, Architecture, and Storage (NAS 2010).

[20] Lotfi Ben Othmane, Ruchith Fernando, RohitRanchal, Bharat Bhargava, Eric Bodden, "Likeli-hoods of Threats to Connected Vehicles," International Journal of Next-Generation Computing, Vol. X, No. X, 07 2014.

[21] Dorothy J. Glancy, "Privacy in Autonomous Vehicles," Santa Clara Law Review, Vol. 52, No. 4 Article 3, December 14, 2012.

[22] Gene Carter, "Privacy in V2V communications: Is somebody watching you?," Security Innovation, May 18th, 2015.

[23] Gene Carter, "V2X technology makes cars safer," Embedded Computing Design, April 10th, 2015.

[24] Mihajlovic R, Mihajlovic A., “Operating Systems Security; The First Cut,” Soft Electronics, New York, May 2015, ISBN-978-194327525-0, pp.256-285.

[25] Matthew Jensen, “How To Track Your Vehicle on The Cheap, Using Your Smartphone?” Study Lifestyle, August 9, 2016.

[26] Schroeder, M., Saltzer, J., “A Hardware Architecture for Implementing Protection Rings.” Communications of the ACM, Vol. 15, No. 3, 1972.

[27] David T. Rogers, "A Framework for Dynamic Subversion," Thesis, Monterey, California. Naval Postgraduate School, June 2003.

[28] Laura Ionita,“Connectivity shifts the power in the automotiveindustry,” Tuck School of Business at Darmouth, Galssmer/McNamee, Center for Digital Strategies, T’15, March 28, 2015.

[29] Lizzie Stromme, "Putin's official car involved in horror crash – killing leader's 'favourite' driver," Express, Sep 6, 2016.

[30] Kim Zetter, "An Unprecedented Look at Stuxnet, the World’s First Digital Weapon," Wired Magazine, 11.03.14.