# Designing security for in-vehicle networks: a Body Control Module (BCM) centered viewpoint

Bogdan Groza, Horaţiu-Eugen Gurban and Pal-Ştefan Murvay
*Faculty of Automatics and Computers*
*Politehnica University of Timisoara, Romania*
*Email: bogdan.groza@aut.upt.ro, horatiu.gurban@gmail.com, stefan.murvay@gmail.com*

*Abstract*—**The overabundance of attacks reported on in-vehicle networks triggered reactions from both the academic research communities and industry professionals. However, designing security for in-vehicle networks is a challenging task and it is yet unclear to what extent current proposals are suitable for real world vehicles. In this work, we advocate the use of a top-down approach in which we analyze the functionalities along with reported attacks. Due to the abundance of in-vehicle services and the associated large number of Electronic Control Units (ECUs), we center our analysis on a key subsystem from the car: the Body Control Module (BCM). The rationale behind choosing this particular module comes from at least three key factors: i) a large number of components that are directly linked to the BCM were target of previously reported attacks (e.g., keys and electronic immobilizes, tire sensors, diagnostic ports, etc.), ii) by design, body components are generally exposed to the outside and it is reasonable to assume that adversaries will frequently have access to peripherals controlled by the BCM, iii) the BCM controls subsystems that are both attractive from an economic perspective (e.g., access to the car), or from a safety perspective (e.g., seat-belts, lights, etc.). Our discussion is entailed by a concrete analysis of the risks of reported attacks and preferable security designs.**

## 1. Introduction

The insecurity of modern cars was decisively proved by the recent comprehensive analysis of vehicle's attack surfaces from [4] and [17]. Currently there are several academic research proposals for securing in-vehicle communication networks, e.g, the CAN bus (Controller Area Network), while the industry recently started to include interfaces for cryptographic primitives in automotive standards, e.g., the AUTOSAR Crypto Abstraction Library and Crypto Service Manager [1], [2]. Still, there are no real-world deployments for cryptographic protocols in cars. This leaves at least some uncertainties over how well studied cryptographic protocols will be embedded in intra-vehicle networks.

Modern vehicles are host to a number of subsystems and functionalities that rely on dozens of ECUs. In large, these subsystems can be grouped in the following categories:

*i)* *body* related subsystems that are responsible for various functionalities related to car access, windows, doors, the diagnostic interface, Heating Ventilation and Air Conditioning (HVAC), etc.,

*ii)* *chassis* related subsystem which are responsible for braking, stability control, steering, etc., and a high number of safety related tasks for vehicle driving, we also include here the Advance Driver Assistance Systems (ADAS),

*iii)* *powertrain and transmission* subsystems that are responsible with the ignition, traction control and a number of tasks that can improve on fuel economy, $CO_2$ emissions, etc.,

*iv)* *infotainment and telematics* subsystems that are responsible for offering an enjoyable user experience by connectivity with user-held devices, e.g., mobile phone, tablets, etc. but also facilitating remote vehicle diagnosis via mobile telecommunication technologies, e.g., 3G.

Intuition suggests that attacks related to *chassis, powertrain and transmission* would have a more critical impact, but as we advocate later, it seems that these subsystems would be easier to isolate from outsiders. The rationale behind choosing the Body Control Module (BCM) as center of our security analysis comes from several key factors which we now enumerate. There are several security appealing facts behind the BCM and related subsystems:

*i)* A large number of components that are directly linked to the BCM were targets of previously reported attacks. Car keys and vehicle immobilizers are connected to the BCM and they are the traditional attack interface if we consider car theft. There is abundant research on hacking car keys and electronic immobilizers [28], [29], [8], [27], [25], [14]. To these one can add the reported attacks on wireless tire sensors [15] and the interest in designing security for these sensors [30]. Moreover, many of the previously reported attacks were also mounted by using the On-board diagnostics port (OBD) [4] which is a mandatory functionality implemented by all ECUs in the car. The BCM module is in many architectures the bridge between the external diagnosis tool and the CAN bus to which other ECUs are connected.

*ii)* By design, body components are always exposed to the outside and it is reasonable to assume that adversaries will frequently have access to peripherals controlled by BCMs. It is harder or even impossible to assure security by isolation or tamper resistance for devices that are an intrinsic part of the car body and thus are closer to the exterior. One can imagine that an adversary (e.g., assume the valet that parks or washes the car) may have difficulties in accessing certain parts of the engine or gear-box but it may be easier to tamper with electronic parts that are located inside mirrors, doors, etc.

*iii*) There are a number of safety and economic factors that make the BCM an attractive attack point. It is clear that car theft always raised financial interests but on the other hand disabling mirrors or lights (when driving at night) may have disastrous consequences.

By no mean we intend to minimize the role of the other subsystems. But the above arguments help us in building the case for the vehicular BCM. We do imagine that our study will provide useful ideas for the security designs in other subsystems as well.

## 2. BCM architecture, functionalities and practical embodiments

In the next paragraphs we try to give a brief overview on current BCM architectures and the associated functionalities.

### 2.1. Generic view of a BCMs network topology

The BCM regularly communicates with a large number of sensors, actuators and ECUs. General-purpose input/output (GPIO) pins are used for communicating with sensors and actuators. The only kind of security that can be assured on these lines is by redundancy. Communication with other embedded devices is done via communication layers such as:

- *LIN (Local Interconnect Network)* a cheap serial communication interface based on a master-slave architecture that reaches speeds of up to 20 kbps. Intended to assure connectivity between various peripheral sensors and actuators for doors, windows, etc.,
- *CAN (Controller Area Network)* a two wire broadcast bus that has a fault tolerant low-speed version which operates at 125kbps and a high-speed version that operates at up to 1Mbps. *CAN-FD (CAN with Flexible Data-Rate)* was designed as replacement for CAN and allows a bandwidth of 2.5 Mbps.
- *FlexRay* is as a faster, more reliable but also more expensive alternative to CAN that can reach up to 10Mpbs. Some projected this bus to be at the heart of future cars, but now some predictions go toward automotive grade Ethernet, i.e., BroadR-Reach.

None of these communication layers has any kind of security except for standard CRC codes that protect against regular transmission errors. Consequently, we cannot currently assume that these lines are secure. We can however predict that in the short-term future they will be secured as there are continuous efforts for designing security for in-vehicle networks.

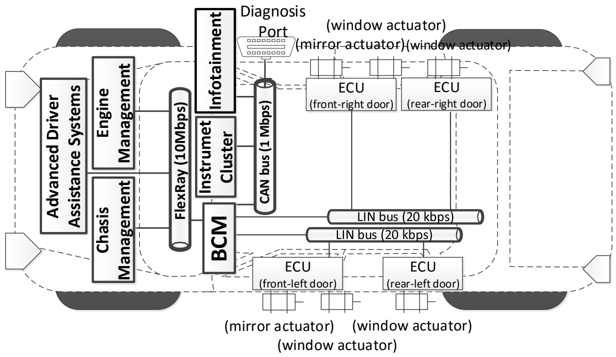

Figure 1. Suggestive depiction of in-vehicle subsystems and connectivity

### 2.2. BCM associated roles and functionalities

The BCM is the main controller for body electronics covering a high number of functionalities: interior and external lighting control, secure entry, centralized door locking, power seats, power windows, wipers, power mirrors and HVAC control. The increasing number of comfort, secure access and safety features that are integrated in current vehicles made the BCM one of the nodes with the highest information sharing needs, so a natural evolution of this node into a central gateway was inevitable. The functionality implemented by body electronics varies based on the auto vehicle class, trim level (level of equipment) and market specifics, European models implementing more features than the US counterpart [26]. Beside the BCM name, different terminology is also used among the car makers to define the ECU that controls the body subsystems: General Electronic Module (GEM), Central Control Unit (CCU) and Central Control Module (CCM) [6], System Acquisition/Activation Modules (SAM-R/D rear/driver Mercedes C, E-Class).

ARCHITECTURES. The functionalities integrated in BCMs depend on the type of architecture employed by the automotive car maker. Two types of architectures are currently considered in the automotive industry: centralized and distributed architectures [19]. Centralized architectures have a lower number of controllers, in this case each one implements a higher number of functionalities, each one being connected to a higher numbers of sensors/actuators. The wiring harness complexity is increased, consisting mainly of electrical wiring for sensors and actuators. In distributed architectures a higher number of controllers are employed, each implementing a subset of functionalities. In the centralized architecture the BCM records the information from digital/analog sensors and actuators controls directly. A high number of analog and digital I/O have to be considered when choosing the microcontroller. When a distributed architecture is employed the car maker has to choose how to connect the distributed controllers - in this case a more complex network topology has to be developed.

Features like self diagnosis, reporting, software updating, parametrization are not specific to the BCM module, being encountered in the vast majority of automotive ECUs. Some of these features are now briefly discussed, providing a common ground of understanding, pointing out the exposed vulnerabilities and presenting reported attacks targeting the BCM.

DIAGNOSTICS SERVICES AND THEIR IMPACT ON SECURITY. The Diagnostics Services are used mainly in workshops for: fault identification (including contextual information), software update, parametrization, calibration and identification of irregular conditions. Currently two diagnosis protocol are used: the Key Word Protocol (KWP, ISO 14230-3) and the Unified Diagnostic Services (UDS, ISO 14229-1 and UDS on CAN ISO 15765-3). The increased number of functionalities implemented using ECUs in the modern automobiles is reflected by a large number of diagnosis services that are used in the life-cycle stages of the automobile: software development, assembly lines, workshops, safety inspection programs and accident investigations. The role of a tester can be assumed by any compromised ECU, OBD connected device or a controller connected on the target CAN network.

Some of the common Diagnosis services that are used to take control of the ECU functionalities and are also relevant from a security perspective include: Read/Write memory by address/identifier (0x22,0x23,0x2E,0x3D ), Device Control/Input-Output Control (0x2F), Request Upload/Download (0x34), Security Access (0x27), Routine Control (0x31), Tester Present (0x3E), Control DTC Settings (0x85). Unfortunately, these services can be used extensively as attack vectors. Since they are all legal and required functionalities, the only security mechanism that can be used is the correct identification and authorization of the device (this can be built with standard cryptographic techniques). Several BCM attacks, using the diagnosis services have been reported: read the hard-coded re-flashing keys from the ECU without authenticating [17], stop the brake lights, headlights and HVAC, activate/deactivate the horn, lock/unlock the doors [17].

The Device Control Service (0x2F) is used to override the normal behavior of the ECU. This is intended to be used in development/workshops to test the ECUs outputs. An attack using the device control commands was presented in [17]. The attack was accomplished by fuzzing the Device Control Service commands and a number of actions related to the BCM module where controlled by means of an external device since no authentication is required, these include [17]: unlock all doors, disable the headlights in auto light control mode, turn off the auxiliary lights, disable the window and key lock relays, turn off the brake/auxiliary lights, etc.

FAILURE DIAGNOSIS. The current regulations demand that the systems and components which (in case of malfunction) can lead to an increased of toxic gas emission have to be monitored. The legislation also stipulates that it is mandatory to monitor the electrical functions and to implement a plausibility check for sensors and actuator functions [24]. Failure-diagnosis refers to fault detection with the remark that contextual information regarding the underlying cause can be also retrieved [18]. The extended information is used during software development, verification and validation stages, and also in vehicle repair shops when the cause of a failure needs further investigation.

Fail-safe actions are implemented for critical events, to mitigate the associated risks and prevent further damages [7]. The actions vary from just recording the DTC occurrences, to limiting the set of functionalities (e.g., limp-home mode) or inhibiting them completely. The DTCs are monitored at start-up, periodically or when some conditions occur, when qualification conditions happen the DTC can trigger the transmission of a CAN frame that will display this information on the electronic instrument cluster (activate the warning lamps or display the fault). The gateway role of the BCM, when tampered with, could provide the driver false information regarding the status of the DTCs - this is relevant from a security perspective as it may lead to further actions with more serious consequences. Another issue can rise from the fact that some systems functions are based on other subsystem information, a DTC falsely reported by a module can lead to inhibition of some functionalities for other modules.

The Diagnostics Services (UDS/KWP) provide subservices that can be used to check the fault conditions (Clear Diagnostic Information, Read DTC Information) but also for modifying the DTC manager implicit behavior: inhibit the monitoring or modify the thresholds values (Control DTC Settings, Read/Write Data By Identifier/Address).

The BCM, monitors a high number of sensors and switches and controls a high number of actuators, transmitting part of the monitored or processed data to other ECUs. Deactivating the hardware DTC monitoring, e.g., short circuit, open circuit, leakage to plus/minus, can lead to hazard situations. Tampering the fault manager can also lead to improper behavior of critical safety systems, e.g. buckle switch error not detected.

XCP. The Universal Measurement and Calibration Protocol (XCP) was standardized by ANSAM (Association for Standardisation of Automation and Measuring Systems) being used for writing parameter calibration values and for acquiring ECUs internal parameters at runtime [23]. XCP has a two-layer structure: transport layer and protocol layer. Based on the transport layer used, the protocol is referred as XCP on CAN, CAN FD, SPI, SCI, Ethernet, USB and FlexRay. None of the attacks reported so far, have been accomplished by using the XCP. Being able to have read/write access to ECU's memory and to reprogram the ECU makes any ECU, which have implemented XCP, a possible attack target.

BCM'S IMPACT ON THE EVENT DATA RECORDER(EDR) INFORMATION. The EDR records information in pre-crash, crash, after crash events, the recorded information being in average less than 30 seconds [13], in this case accurate and reliable information regarding the timing, chronology of events can be retrieved after the crash situation. The EDR information are used in modern vehicle crash investigations/ reconstructions and in legal proceedings. The BCM gateway role can also have a significant importance for the EDR because when tampering the BCM module (e.g., malicious modification of the frames that have to be sent to the EDR's network) inconsistency between EDR recordings and the real contextual data will occur, misleading on the exact cause of certain events. Safety critical information such as the state of buckle switches is provided by the BCM, thus the active and passive safety functions can be severely compromised. For example the reversible seat belt pretension ECU will not impose a correct belt tension in a pre-crash situation by belt tensioning with motor/explosive charge. When the seat belt pre-tensioner and load limiter are employed it is estimated that the fatality risk in case of a crash is reduced by 12.8% [16]. The state of buckle switches and the traceability of safety mechanisms is relevant information in the aftermath of any severe incident.

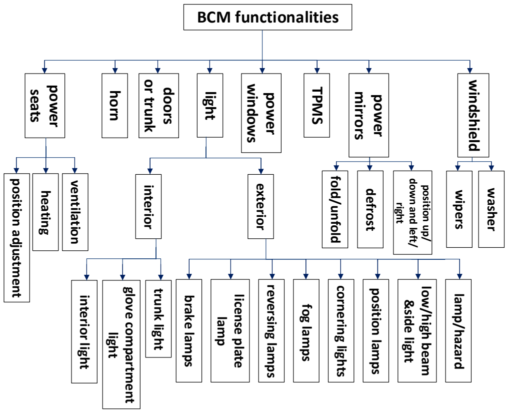

Figure 2. Brief overview of BCM functionalities

### 2.3. Embedded platforms behind BCMs

According to [5], the first five suppliers of automotive semiconductor market are: Renesas, Infineon, STMicroelectronics, Freescale and NXP. Table 1 provides a brief overview of the main characteristics of the microcontrollers which are suggested by these semiconductor companies to be used as BCM controllers. The suggested microcontrollers use 32bit architecture, with two or three cores. Some multi-core architectures feature multiple instance of the same core type with clock speeds in the 100-160MHz range while others come with different core types with some reaching operation speeds of up to 80MHz.

The multi-core architectures proposed by semiconductor manufacturers are motivated by the double role played by the BCM controller, main controller for body functions and network gateway, each core being associated with one functionality. These controllers target the higher end cars class due to the large number of CAN channels (between 6 and 8), LIN channels (between 10 to 18) and the presence of FlexRay and ETHERNET capabilities. The main conclusion is that BCM modules get hold of sufficient computational resources for implementing more demanding security functions, e.g., cryptography.

TABLE 1. CHARACTERISTICS OF SOME COMMONLY USED DEVICES FOR BCM MODULES

| Manufacturer | CPU characteristics | Peripherals microcontroller |
|---|---|---|
| Renesas | RH850 F1H<br>CPU: 2 X RH850G3<br>32bit, 120 MHz<br>Program Flash: 6MB<br>EEPROM: 64 KB<br>SRAM: 576 KB | I/O Port: 218; LIN Master: 12 ch.<br>LIN/UART: 6 ch.; CAN: 7 ch.<br>FlexRay: 1 ch.;Ethernet: 1 ch.<br>HW Security Module (ICU-M) |
| Freescale | MPC564xB-C family<br>MPC5646C<br>CPU: e200Z4, 32bit, 120MHz<br>e200Z0, 32bit, 80MHz<br>Program Flash: 3 MB<br>EEPROM: 64 KB<br>SRAM: 256 KB | GPIO: 199; LIN: 10 ch.<br>CAN: 6 ch.; FlexRay: 1 ch.<br>Ethernet: 1 ch.<br>Secure key storage<br>AES-128 en/decryption, ECB/CBC<br>Authentication with AES-128 CMAC<br>SHE Secure boot protocol<br>TRNG and AES-128 based PRNG |
| Freescale | MPC5748G family<br>CPU:2x e200Z4,32b,160MHz<br>1 x e200Z2, 32bit, 80MHz<br>Program Flash: 6 MB<br>Data Flash: 192 KB<br>SRAM: 768 KB | LINFlex: 18 ch.<br>CAN: 8 ch. (CAN FD support)<br>FlexRay: 1 dual-channel FlexRay<br>Ethernet: 2 ch.<br>One Secure Digital HW Controller |
| Infineon | XC2200 family<br>XC2299H-200FxL,<br>scalable 16/32bit,100 MHz<br>Program Flash: 1.6 MB<br>SRAM: 112 KB | GPIO : 150; LIN/UART : 10 ch.<br>CAN: 6 ch.; FlexRay: 2 FlexRay Nodes<br>Ethernet: none |
| STMicroelectronics | SPC56ECxx family<br>SPC56EC74L7<br>CPU: e200Z4d, 32bit, 120MHz<br>e200Z0h, 32bit, 80MHz<br>Program Flash: 3 MB<br>Data Flash: 64 KB<br>SRAM: 256 KB | GPIO : 199; LIN/UART: 10 ch.<br>CAN: 6 ch.;<br>FlexRay: 1 dual channel FlexRay<br>Ethernet: 1 ch.<br>Cryptographic Services Engine (CSE),<br>AES-128 en/decryption, CMAC auth.,<br>Secured device boot mode |

## 3. Risk assessment for the BCM

In order to quantify the risks associated to each attack, we begin with an overview of the factors that we consider for assessing the impact and likelihood of the intrusion. Then we provide a risk based classification of the reported attacks in the light of this framework. Finally, we discuss countermeasures.

### 3.1. Evaluation framework

We partly base our assessment of security risks on the methodology from [9] and [3]. To this we do add some particular coefficients and flavours to each of the components in the evaluation of the impact and likelihood of the attack.

The risk of an threat is commonly evaluated based on two components: the impact of the threat and the difficulty in mounting the attack. The *impact of the threat* can be further refined along the following factors:

- *safety* - the impact of the attack on the safety of vehicle occupants as well as on other traffic participants,
- *financial* - the cost associated to the damage,
- *privacy* - the privacy of the vehicle owner and occupants,
- *operational* - the interference with vehicle's normal behavior,

The *likelyhood of the attack* can be further refined along the following lines:

- *time* - the time required to identify a vulnerability,
- *expertise* - the level of knowledge required to perform the attack,
- *insider knowledge* - the amount of insider information that is needed,
- *window of opportunity* - the number of attempts required to mount the attack,
- *equipments* - the physical devices that are required to mount the attack.

Additionally, in [3] the *legal* impact as well as the *reputation* damage are considered. We found the classification and the corresponding risk result to be sufficiently accurate for our study even in the absence of these factors. Moreover, legal implications are not always clear and reputation damage seems to be hard to quantify in the light of recent incidents (e.g., the VW emission scandal).

Based on the above factors the impact can now be computed by summing over the product of each factor with the corresponding coefficient. A similar procedure is adopted for the difficulty of the attack, which leads to the following two equations:

$$\mathbb{I} = \alpha_{Sf} I_{Sf} + \alpha_{Fin} I_{Fin} + \alpha_{Prv} I_{Prv} + \alpha_{Op} I_{Op}$$

$$\mathbb{D} = \alpha_T D_T + \alpha_{Ex} D_{Ex} + \alpha_{In} D_{In} + \alpha_W D_W + \alpha_{Eqp} D_{Eqp}$$

Finally, we define the risk of the attack as the product of the impact with the inverse of the difficulty of the attack

$$\mathbb{R} = \mathbb{I} \times \mathbb{D}^{-1}$$

We proceed to a more practical analysis with concrete numerical values in the next subsection.

### 3.2. Risk analysis based on reported attacks

In Table 2 we define the scale for the impact factors, then Table 3 does the same for the difficulty factors, these values are similar to the ones in [9] and [3]. Choosing specific coefficients for each of these factors may be a harder decision, we do present our choice in Table 4. In general we assume that safety plays the more critical role, hence the highest coefficient, i.e., 8, then the financial factors prime followed by the operational impact and last comes privacy. As for the difficulty, we did assume that the window of opportunity is the most important, again scored at 8, followed by the need for dedicated equipments, insider knowledge, expertise and time. All coefficients are obtained by successive halving from the highest one; this decision was driven by our intuition on the associated risks.

TABLE 2. Attack Severity Classification and Rating

| | Safety | Privacy | Financial | Operational |
|---|---|---|---|---|
| 0 | no injury | none | none | none |
| 1 | light | anonymous data | 10$ | indiscernible |
| 2 | severe | driver/vehicle identification | 100$ | discernible but insignificant performance impact |
| 3 | life threatening | driver/vehicle tracking | 1.000$ | noticeable impact |
| 4 | fatal | driver/vehicle tracking on multiple vehicles | 10.000$ or above | significant impact for multiple vehicles |

TABLE 3. Attack Potential Classification and Rating

| | Time | Expertise | Insider knowledge | Window of opportunity | Dedicated equipment |
|---|---|---|---|---|---|
| 0 | days or less | user | no knowledge | unlimited | none |
| 1 | week or less than a month | technician | public domain | large | standard/ easily accessible |
| 2 | month or less than a year | proficient | basic insider knowledge (e.g., mechanic) | medium | off-the shelf, costs < 100$ |
| 3 | expert | proficient | insider information (e.g., designer) | small | off-the shelf, costs <1000$ |
| 4 | many years, not practical | multiple ex- perts | specialized/multi insider information (e.g., designers, testers) | real- time | specialized, costs >1000$ |

TABLE 4. Coefficients for Impact and Difficulty

| $\alpha_{Sf}$ | $\alpha_{Fin}$ | $\alpha_{Prv}$ | $\alpha_{Op}$ | $\alpha_T$ | $\alpha_{Ex}$ | $\alpha_{In}$ | $\alpha_W$ | $\alpha_{Eqp}$ |
|---|---|---|---|---|---|---|---|---|
| 8 | 1 | 4 | 2 | 1 | 2 | 2 | 8 | 4 |

We made a list of potential attacks on BCMs by surveying the available literature on automotive attacks and extracting the ones that target functionalities which are associated to the BCM. Table 5 presents this list of attacks along with the required access needed for achieving each of them. Table 5 includes the computed value for the risk of each of the attacks.

A brief inspection of Table 5 shows that the attacks on wireless keys are actually the most irrelevant, despite the great impact in the media, as they lead to no injuries. The highest risk is given by the attacks that disable certain subsystems of the car, especially when this is remotely done (of course, this is due to the highest impact on safety).

### 3.3. Proposed security approach

The risk analysis in section 3.2 shows that in general attacks related to body components do not immediately pose

TABLE 5. Risk score calculated for reported attacks on vehicle body modules

| Target system | Attack | Access | Impact factors | | | | $\mathbb{I}$ | Difficulty factors | | | | | $\mathbb{D}$ | $\mathbb{R}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | $I_{Sf}$ | $I_{Fin}$ | $I_{Prv}$ | $I_{Op}$ | | $D_T$ | $D_{Ex}$ | $D_{In}$ | $D_W$ | $D_{Eqp}$ | | |
| **Electric window lift** | Open window - sniff and replay attack (simulation CANoe) [11] | CAN | 3 | 0 | 2 | 2 | **36** | 0 | 2 | 1 | 0 | 2 | **14** | **2.57** |
| | DoS - for each command send opposite command message [12] | CAN | 3 | 0 | 2 | 2 | **36** | 1 | 2 | 1 | 0 | 2 | **15** | **2.40** |
| | Disable window relays [17] | OBD | 3 | 0 | 2 | 2 | **36** | 0 | 2 | 1 | 0 | 2 | **14** | **2.57** |
| **Windshield wipers** | Turn wipers on continuously [17] | OBD | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| | Turn fluid shot continuously [17] | OBD | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| | Force wipers off & shots fluid continuously [17] | OBD | 3 | 0 | 0 | 4 | **32** | 0 | 2 | 1 | 0 | 2 | **14** | **2.29** |
| **Exterior lights** | All lights off (brake and auxiliary) [17] | OBD | 3 | 0 | 4 | 4 | **48** | 0 | 2 | 1 | 0 | 2 | **14** | **3.43** |
| | All auxiliary lights off [17] | OBD | 3 | 0 | 4 | 4 | **48** | 0 | 2 | 1 | 0 | 2 | **14** | **3.43** |
| | Disable headlights in auto light control [17] | OBD | 3 | 0 | 4 | 4 | **48** | 0 | 2 | 1 | 0 | 2 | **14** | **3.43** |
| | Turn headlights on or off while in auto light control [21] | OBD Diag | 3 | 0 | 4 | 4 | **48** | 0 | 2 | 1 | 0 | 2 | **14** | **3.43** |
| **Interior lights** | Control dome light brightness [17] | OBD | 3 | 0 | 4 | 2 | **44** | 0 | 2 | 1 | 0 | 2 | **14** | **3.14** |
| **Trunk door** | Pop open [17] | OBD | 0 | 0 | 2 | 2 | **12** | 0 | 2 | 1 | 0 | 2 | **14** | **0.86** |
| **Doors** | Unlock all (while at speed) [17] | OBD | 3 | 0 | 0 | 2 | **28** | 0 | 2 | 1 | 0 | 2 | **14** | **2.00** |
| | Lock/Unlock car [17] | OBD | 3 | 0 | 2 | 2 | **36** | 0 | 2 | 1 | 0 | 2 | **14** | **2.57** |
| | Continuously activate lock relay [17] | OBD | 3 | 0 | 2 | 2 | **36** | 0 | 2 | 1 | 0 | 2 | **14** | **2.57** |
| | Lock/unlock all while driving [21] | OBD Diag | 3 | 0 | 0 | 2 | **28** | 0 | 2 | 1 | 0 | 2 | **14** | **2.00** |
| **Horn** | Activates permanently [17] | OBD | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| | Change Frequency [17] | OBD | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| | Turn horn on and off [21] | OBD Diag | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| **Cluster instrument** | Control brightness [17] | OBD | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| | Falsify speedometer reading [17], [21] | OBD | 3 | 0 | 4 | 2 | **44** | 0 | 2 | 1 | 0 | 2 | **14** | **3.14** |
| | Speedometer drops to 0 (DoS to/from ECM) [17] | OBD | 3 | 0 | 4 | 2 | **44** | 0 | 2 | 1 | 0 | 2 | **14** | **3.14** |
| | Panel freezes (DoS to/from BCM) [17] | OBD | 3 | 0 | 4 | 2 | **44** | 0 | 2 | 1 | 0 | 2 | **14** | **3.14** |
| | Falsify fuel level [17] | OBD | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| | Control various fields on the dashboard [10] | OBD | 3 | 0 | 4 | 2 | **44** | 0 | 2 | 1 | 0 | 2 | **14** | **3.14** |
| | Force odometer value increase [21] | OBD | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| | Falsify fuel level [21] | OBD Diag | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| **Smart Junction Box** | Shut down causing several systems (lights, radio, HVAC etc.) to stop [21] | OBD Diag | 4 | 0 | 4 | 2 | **52** | 0 | 2 | 1 | 0 | 2 | **14** | **3.71** |
| | Start reprogramming causing interior lights to flash [21] | OBD Diag | 4 | 0 | 4 | 2 | **52** | 0 | 2 | 1 | 0 | 2 | **14** | **3.71** |
| **Remote disable system** | Disable cars and sound horn continuously [20] | Main remote access system | 4 | 0 | 4 | 2 | **52** | 2 | 3 | 2 | 0 | 0 | **12** | **4.33** |
| **Remote Keyless Entry** | Breaking KeeLoq authentication by key recovery - cryptanalysis: known plaintexts, slide attack & meet-in-the-middle [14] | Key RF range | 0 | 2 | 2 | 0 | **10** | 2 | 3 | 1 | 0 | 0 | **10** | **1.00** |
| | Breaking KeeLoq authentication by key recovery (both remote transmitter and manufacturer key) - side channel: DPA, SPA [22] | Key RF range | 0 | 2 | 2 | 0 | **10** | 2 | 3 | 1 | 0 | 0 | **10** | **1.00** |
| | Jamming attack - lock signal is jammed and car remains open [8] | Car RF range | 0 | 2 | 2 | 0 | **10** | 0 | 1 | 0 | 0 | 3 | **14** | **0.71** |
| | Replay attack - unlock message is recorded and replayed [8] | Key or car RF range | 0 | 2 | 2 | 0 | **10** | 1 | 2 | 1 | 3 | 3 | **43** | **0.23** |
| **Passive Keyless Entry** | Wired relay attack - open car door & start engine [8] | Key or car RF range | 0 | 2 | 4 | 0 | **18** | 1 | 2 | 1 | 3 | 3 | **43** | **0.42** |
| | Wireless relay attack - open car door & start engine [8] | Key or car RF range | 0 | 2 | 4 | 0 | **18** | 1 | 2 | 1 | 3 | 3 | **43** | **0.42** |
| **Immobilizer** | Tracking of the key fob using Atmel immobilizer protocol stack [27] | Key RF range | 0 | 2 | 0 | 0 | **2** | 2 | 3 | 1 | 2 | 3 | **38** | **0.05** |
| | DoS Atmel immobilizer protocol stack - Overwrite keys in open and secure mode => key will not work with car [27] | Key RF range | 0 | 2 | 0 | 0 | **2** | 2 | 3 | 1 | 0 | 3 | **22** | **0.09** |
| | Relay attack on Atmel immobilizer protocol stack [27] | Key or car RF range | 0 | 2 | 4 | 0 | **18** | 1 | 2 | 1 | 3 | 3 | **43** | **0.42** |
| | Replay attack on authentication for keys based on Atmel immobilizer protocol stack [27] | Key or car RF range | 0 | 2 | 4 | 0 | **18** | 1 | 2 | 1 | 3 | 2 | **39** | **0.46** |
| | Spoofing attack to lock the EEPROM in Atmel immobilizer protocol stack [27] | Key or car RF range | 0 | 2 | 4 | 0 | **18** | 2 | 3 | 1 | 0 | 2 | **18** | **1.00** |
| | Retrieve secret key and start engine for Hitag2-based transponders [28] | Key or car RF range | 0 | 2 | 4 | 0 | **18** | 3 | 3 | 1 | 0 | 2 | **19** | **0.95** |
| **Car Alarm** | Honk horn [17] | OBD | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| **Key lock** | Disable relays [17] | OBD | 0 | 0 | 0 | 0 | **0** | 0 | 2 | 1 | 0 | 2 | **14** | **0.00** |
| **HVAC** | Turn fans, A/C or heat on/off [17] | OBD | 0 | 0 | 0 | 2 | **4** | 0 | 2 | 1 | 0 | 2 | **14** | **0.29** |
| **TPMS** | Tracking automobiles by sensor IDs [15] | Car RF range | 0 | 4 | 0 | 0 | **4** | 1 | 2 | 1 | 1 | 2 | **23** | **0.17** |
| | Packet spoofing from a neighbor car - fake low tire pressure warning [15] | Car RF range | 0 | 0 | 2 | 0 | **8** | 1 | 2 | 1 | 1 | 2 | **23** | **0.35** |
| | Battery drain [15] | Car RF range | 0 | 0 | 1 | 2 | **8** | 1 | 2 | 1 | 1 | 2 | **23** | **0.35** |
| | Crash TPMS ECU - repeated spoofing [15] | Car RF range | 0 | 0 | 2 | 2 | **12** | 1 | 2 | 1 | 1 | 2 | **23** | **0.52** |

safety risks but the situation can drastically change in certain circumstances. For example disabling the exterior lights will likely have no impact during day in proper illumination conditions, but it will certainly have fatal consequences during night. Given this potential risk escalation it is clear that designing security for BCM units is necessary.

To obtain a clearer image on the proper designs, we begin with a brief classification of the attacks encountered so far. Currently reported attacks can be grouped in the following categories:

- **A1**. Attacks due to *misuse of various services*, e.g., connectivity to the OBD port, telematics or infotainment followed by the injection of malicious messages [4], [17].
- **A2**. Attacks that *exploit the lack of cryptographic security* on various wired communication buses, e.g., CAN, FLexRay, etc. as well as wireless interfaces [4], [17], [15]. These attacks are distinct from the previous class of attacks since there is no exploitation of some desired functionality, i.e., the adversary simply acts as a genuine device on the communication bus.
- **A3**. Attacks that *exploit existing cryptographic vulnerabilities* on wireless channels, e.g., keys, sensors, etc., [28]. These attacks take place only on interfaces that are presumably protected by standard cryptographic mechanisms.

Having the clearer image over the attack potential, we can now discuss countermeasures. Intuition suggests that *chassis*, *powertrain and transmission* related subsystems will play the more critical role in assuring the safety of passengers and other traffic participants. However, one significant question that arises is whether communication between ECUs related to these subsystems should be secured by cryptography (which causes high communication and computational overheads) or these subsystems should be isolated. As security researchers we do perfectly understand that security through isolation is in general not a correct design decision. But if these safety critical subsystems are not isolated from the outside, at least to some extent, it will not be possible to give safety assurances. For example, even if these subsystems would be purely mechanical (i.e., no embedded networks or ECU) or communication would be perfectly secured by cryptography one could always insert a device which cuts wires to the brakes or pipes that carry fuel to the cylinders. Such incidents are clearly not frequent and they do not appear to be a threat to the common car owners. It is the possibility that an adversary can hack a car from remote which frightens us, e.g., by plugging a simple devices on the diagnostic port, or establishing a connection to the telematics unit. To achieve this, it is clear that connectivity between *body*, *infotainment* and/or *telematics* (which are the only units connected to the outside) and the corresponding *chassis*, *powertrain and transmission* must be exploited. This leads us to the impression that basic network mechanisms, e.g., firewalls, should be employed to block certain messages to be routed from interfaces to the outside, e.g., a cd/usb-player, to the safety critical powertrain subsystems. Since the *infotainment* subsystem seems the most prone to security issues (at least due to the insecurity of an operating system that connects to various insecure gadgets) the complete detachment of it from interfering with other sub-systems is a must.

Cryptographic mechanisms should be present whenever possible to implement. Redundancy is also necessary, but this is already well studied in automotive design. Consequently, we advocate for the use of the following three types of countermeasures:

- **C1**. Standard *firewall functionalities* that will block messages unrelated to the intended device are a must. If by design there are functionalities that can affect other components, access to these should be granted only through proper *authorization and authentication mechanisms*.
- **C2**. Protocols used by all ECUs that implement chassis, body or power-train functions that are safety critical must be protected by *cryptographic authentication protocols*. There are plenty of academic proposals and there are also ongoing efforts on the industry's side for standardizing cryptographic interfaces in the AUTOSAR standard [1], [2].
- **C3**. *Redundancy, physical separation and tamper-proofing* must be considered in case when it is not possible to use firewalls or cryptographic security. This seems to be the case for various sensors or actuators as well as ECUs that communicate over low-speed communication buses such as LIN.

As for the attacks that exploit weak cryptographic designs on wireless channels, e.g., keys, sensors, etc., the use of the proper protocol designs will fix the problem. However, these attacks seem to have only financial impact for the moment and do not appear to be safety critical.

Figure 3 depicts the three classes of countermeasures in an environment that is centered around a BCM module. The BCM module acts as gateway and as well as a firewall. The Infotainment unit as well as the Diagnosis port are placed on a distinct CAN bus and the BCM can filter the packets and redirect only legitimate packets to the other buses. In case of the Infotainment unit it is likely that no packet should pass to the other buses, but for the OBD port legitimate tools may receive access if they provide the proper credential by secure authentication protocols. The Engine, Chasis and ADAS related ECUs are separated on a high-speed FlexRay bus where proper cryptographic authentication protocols are used. Finally, the low-power ECUs as well as the sensors and actuators are separated in an area that is secured by isolation. While in Figure 3 we depict a clear separation between the areas, for real-world vehicles due to specific placement of various devices overlaps may be present.

## 4. Conclusion

Insofar security designs addressed mostly communication buses inside the car in the absence of a crisper view of existing functionalities. The BCM (Body Control Module) is a relevant component of current in-vehicle architecture that covers key functionalities that are relevant from a security point of view both as functionality and attack surface. We did advocate the relevance of this component from a

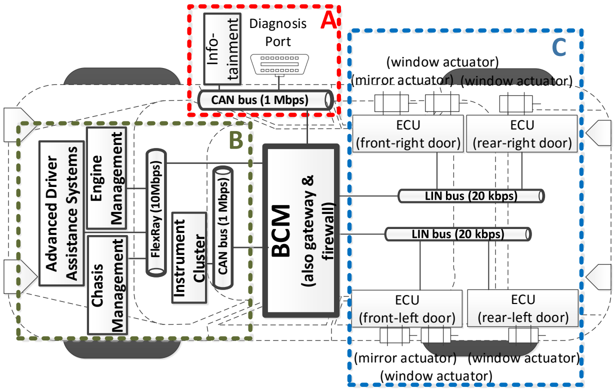

Figure 3. Separation of security designs around the BCM module

risk analysis perspective and discussed on potential security mechanisms. The image that we bring emphasizes on the use of a mixture of mechanisms: firewalls, standard cryptography as well as physical security mechanisms. Clearly, each of these lines requires more in-depth future research which remains within our preoccupations, this work only tried to fix a real-world oriented security viewpoint.

## Acknowledgments

This work was supported by a grant of the Romanian National Authority for Scientific Research and Innovation, CNCS-UEFISCDI, project number PN-II-RU-TE-2014-4-1501 (2015-2017).

## References

[1] AUTOSAR. *Specification of Crypto Abstraction Library*, 4.2.2 edition, 2015.

[2] AUTOSAR. *Specification of Crypto Service Manager*, 4.2.2 edition, 2015.

[3] L. ben Othmane, R. Ranchal, R. Fernando, B. Bhargava, and E. Bodden. Incorporating attacker capabilities in risk estimation and mitigation. *Computers & Security*, 51:41–61, 2015.

[4] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*. San Francisco, 2011.

[5] M. Culver. 2014 automotive semiconductors supplier rankings adjusted based on further analysis, ihs says. Technical report, IHS Press, 2015.

[6] T. Denton. *Automobile electrical and electronic systems*. Routledge, 2012.

[7] J. Erjavec and R. Thompson. *Automotive technology: a systems approach*. Cengage Learning, 2014.

[8] A. Francillon, B. Danev, S. Capkun, S. Capkun, and S. Capkun. Relay attacks on passive keyless entry and start systems in modern cars. In *NDSS*, 2011.

[9] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl. Security requirements for automotive on-board networks. In *Proceedings of the 9th International Conference on Intelligent Transport System Telecommunications (ITST 2009), Lille, France*, 2009.

[10] C. Hoder, T. Sumers, and G. Zulauf. Hot-Wiring of the Future: Exploring Automotive CANs. In *REcon Conference*, 2013.

[11] T. Hoppe and J. Dittman. Sniffing/replay attacks on can buses: A simulated attack on the electric window lift classified using an adapted cert taxonomy. In *Proceedings of the 2nd workshop on embedded systems security (WESS)*, pages 1–6, 2007.

[12] T. Hoppe, S. Kiltz, and J. Dittmann. Security threats to automotive can networks–practical examples and selected short-term countermeasures. In *Computer Safety, Reliability, and Security*, pages 235–248. Springer, 2008.

[13] D. Hynd and M. McCarthy. Study on the benefits resulting from the installation of event data recorders. Technical Report PPR707, Transport Research Laboratory, 2014.

[14] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, and B. Preneel. A practical attack on KeeLoq. In *Advances in Cryptology–EUROCRYPT 2008*, pages 1–18. Springer, 2008.

[15] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *19th USENIX Security Symposium, Washington DC*, pages 11–13, 2010.

[16] C. J. Kahane. Effectiveness of pretensioners and load limiters for enhancing fatality reduction by seat belts. Technical Report Report No. DOT HS 811 835, Washington, DC: National Highway Traffic Safety Administration, 2013.

[17] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, et al. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462. IEEE, 2010.

[18] P. E. Lanigan, S. Kavulya, P. Narasimhan, T. E. Fuhrman, and M. A. Salman. Diagnosis in automotive systems: A survey. *Parallel Data Laboratory Carnegie Mellon University, Pittsburgh*, pages 11–110, 2011.

[19] T. Martinez. Body control module (bcm, 2009.

[20] S. McClure, A. Weimerskirch, M. Wolf, C. Paar, W. Stephan, and S. Goss. Caution: Malware ahead. an analysis of emerging risks in automotive system security. Technical report, McAfee, 2011.

[21] C. Miller and C. Valasek. Adventures in automotive networks and control units. *DEF CON*, 21:260–264, 2013.

[22] C. Paar, T. Eisenbarth, M. Kasper, T. Kasper, and A. Moradi. Keeloq and side-channel analysis-evolution of an attack. In *Fault Diagnosis and Tolerance in Cryptography (FDTC), 2009 Workshop on*, pages 65–69. IEEE, 2009.

[23] A. Patzer and R. Zaiser. *XCP - The Standard Protocol for ECU Development, Fundamentals and Application Areas*. Vector Informatik GmbH, 2014.

[24] K. Reif. *Automotive Mechatronics -Automotive Networking, Driving Stability Systems, Electronics*. Springer Vieweg, 2015.

[25] Y. Shoukry, P. Martin, P. Tabuada, and M. Srivastava. Non-invasive spoofing attacks for anti-lock braking systems. In *Cryptographic Hardware and Embedded Systems-CHES 2013*, pages 55–72. Springer, 2013.

[26] V. Systems. Automotive architectures for interior electronics. Technical report, Vanadium Systems, LLC, 2006.

[27] S. Tillich and M. Wójcik. Security analysis of an open car immobilizer protocol stack. In *Trusted Systems*, pages 83–94. Springer, 2012.

[28] R. Verdult, F. D. Garcia, and J. Balasch. Gone in 360 seconds: Hijacking with hitag2. In *Proceedings of the 21st USENIX conference on Security symposium*, pages 37–37. USENIX Association, 2012.

[29] J. Wetzels. Broken keys to the kingdom: Security and privacy aspects of rfid-based car keys. *arXiv preprint arXiv:1405.7424*, 2014.

[30] M. Xu, W. Xu, J. Walker, and B. Moore. Lightweight secure communication protocols for in-vehicle sensor networks. In *Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles*, pages 19–30. ACM, 2013.