Risk assessment and security countermeasures for vehicular instrument clusters

Eugen Horatiu Gurban, Bogdan Groza and Pal-Stefan Murvay
Faculty of Automatics and Computers, Politehnica University of Timisoara, Romania
Email: {eugen.gurban, bogdan.groza, pal-stefan.murvay}@aut.upt.ro

***Abstract*—The vehicular instrument cluster has the vital task of informing the driver on vehicle status or potential malfunctions. While this role is merely informative, the implications are far reaching as the driver needs to take decisions based on the reports provided by the instrument cluster. Past attacks on instrument clusters were rather concerned with mundane tasks, e.g., mileage modification, but giving false information to the driver on vehicle speed or triggering/hiding relevant alarms may have serious consequences as it can lead to severe traffic accidents. In this work we discuss risks associated to attacker actions on instrument clusters and envision a potential model-based intrusion detection system to detect potential attacks. Rather than advocating a holistic approach, in which security is designed for the entire vehicle network, e.g. CAN or FlexRay, we follow a component-based approach in which particularities of the instrument cluster and redundancy of information are used to detect potential attacks.**

I. Historical background and motivation

The instrument cluster is the driver's main information source on the status of various vehicle components. The first measuring instruments installed in vehicles at the beginning of the 19th century, as standard equipment, were gauges for monitoring oil level, water pressure or coolant temperature [1] at a time when vehicle reliability was the main concern. The speedometer was introduced as a result of the speed limit laws being promulgated in USA (1901). While initially scattered on the dashboard the gauges where clustered as a distinct panel by the 1920s. By the 50s the gauge-based instrument cluster (IC) provided information on speed, battery charging rate, fuel level, oil pressure and coolant temperature while warning lights were introduced only later replacing some of the gauges [2]. Mechanical trip computers (offering information such as average speed/fuel consumption, instant fuel consumption, travelled distance) were introduced in cars around the 60s, being replaced by electronic ones later on. Various types of analog gauges (mechanical and electromechanical) were employed as the complexity of the information system increased: thermal-type gauges, moving iron gauges, air-cored gauges [3]. The first electronic IC equipped the 1976 Aston Martin Lagonda, it used a digital LED instrumentation but the concept did not catch on the market. Analogue style gauges were the norm in the past decades and remain popular even today.

Current IC solutions on the market can be divided into three main categories: i) hybrid implementation with mechanical needle gauges and central add-on display, ii) hybrid implementation with a central gauge surrounded by two LCD displays and iii) full LCD IC implementations. The central add-on display is usually 4-inch small resolution screen, e.g., 270x480 pixels, displaying trip computer functions, navigation, infotainment and configuration information. Solutions with two LCDs with higher resolutions exist as well, while high-end vehicles employ large LCDs (12 inches) at 140 dpi. For high-end vehicles, the IC panel may also provide options to configure and use the infotainment unit (sound, radio, media, telephone, etc.), the navigation system and several driver assistance functions (night vision, parking etc.). Thise historical background suggests an over-increasing role for instrument clusters inside cars. Their dependence on information extracted from the in-vehicle network makes them prone to security attacks. There are several lines of work that decisively proved the insecurity of modern vehicles and instrument clusters were within reach for such attacks [4], [5], [6], [7]. We discuss more on these in a section dedicated to risk analysis. Countermeasures where proposed by numerous lines of work but these employ holistic approaches that secure the entire communication bus rather than addressing a single component. In particular, intrusion detection mechanisms have been recently considered for the CAN(Controller Area Network) bus in [8], [9] and [10]. These lines of work are based on generic mechanisms that hold for all the communication on the bus, e.g., [10] computes the clock-skews of the senders to detect deviations and thus intrusions, [9] uses the entropy of messages while [8] uses cryptographic authentication. In contrast, here we advocate a component-specific approach that uses specific information and redundancies to detect intrusions, this of course does not contradict but complements previous approaches by adding a new layer of defence that can signal new intrusions (e.g., when all other mechanisms are bypassed).

II. Network topologies and device capabilities

The increased number of modules inside a car made it difficult to manage the required amount of point-to-point connections. This lead to the introduction of bus systems that connect the IC with various Electronic Control Units(ECUs)

inside the car. The topology of the bus is relevant in assessing the position of the IC. Nonetheless, the over-increasing functionalities call for more computational power and thus more capable controllers. We make a brief overview on these in what follows.

A. Topologies

A good overview of existing automotive network topologies is presented by Miller and Valasek [7]. We now briefly discuss on different in-vehicle network topologies from various manufacturers emphasizing the positioning of the IC node in relation to other network components. The position of the IC is critical due the fact the IC is linked to a bus where corrupted nodes may exist or outside access may be facilitated via On-board diagnostics (OBD) port.

According to [7] in the *2015 Cadillac Escalade AWD* the IC is connected to the low speed CAN (LS-CAN) bus and the MOST network being in direct contact with traffic from body, comfort, ADAS and multimedia systems, etc. Communication with other subnetworks is assured through the Body Control Module (BCM) which is used as a gateway.

A more complex network example comes from the *2014 Range Rover Evoque* where the IC is directly connected to two CAN buses, one serving the powertrain system while the other is dedicated to comfort and convenience systems. Messages from other subnetworks reach the IC through the main gateway node which is connected to all CAN buses as shown in Figure 1.

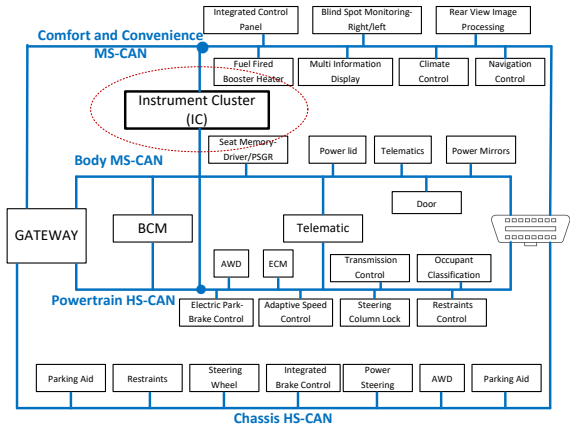


Figure 1. CAN bus topology of a Range Rover Evoque based on [7]

In some cars with less CAN buses the IC is directly connected to a wide range of ECU types. For example, the IC of the *2014 Toyota Prius* is connected to a single CAN bus along with ADAS, safety, powertrain and body control modules. A similar example comes from the *2010 FORD Escape* in which the IC connects directly with two CAN sub networks which also accomodate traffic for ADAS, safety, powertrain, comfort body and multimedia nodes [6]. In newer models from the same manufacturer, like the 2014 Ford Fusion the IC is connected to one CAN sub network which it only shares with the central gateway along with multimedia and comunication systems [7]. Similar IC connectivity can be found in BMW models such as the 2014 BMW 3 Series (F30), BMW X3 (F25) and BMW i12 where the IC is connected through a MOST(Media Oriented Systems Transport) bus to the central gateway, multimedia and communication systems [7].

B. IC functionalities and embedded platforms

Traditionally instrument clusters are equipped with gauges, warning lamps and indicators. Here we just enumerate the most common functionalities since they may be a target for misinforming the driver.

Gauges include indicators for speed, fuel level, engine coolant temperature and the tachometer. Warning lamps are available for low coolant level, ABS system fault, oil pressure low, alternator fault, seat belt not fastened, engine fault, low fuel level, oil pressure, light bulbs failure, open doors/trunk, brake pad wear, low tire pressure, low brake fluid level / fault in brake system. Indicators are available for lights in operation (headlight low/high beams, front/rear fog lights, turn signals), active cruise control, ESP in operation, traction control disabled, parking brake applied, etc.

Advanced driver assistance systems (ADAS) are gaining more popularity on premium vehicles. These systems provide some of the following functionalities: adaptive cruise control, automatic braking, advanced parking assistant, blind spot detection, lane departure warning, lane keeping system, automatic lane change, traffic sign recognition, intelligent headlamp control. These subsystems use the IC to display information regarding status or alerts.

One key information displayed by the instrument cluster is the odometer. The odometer is a standard feature displaying the total distance traveled by a car, additional information can be provided by the trip computer. It initially equipped just the higher-end models but nowadays is a standard function of the IC. It displays mainly the following information: instant/average fuel consumption, trip distance, autonomy with the current fuel. This information was prone to attacks in the past due to the increased reselling value of a second hand car with low kilometer count. In Germany alone it is estimated by the police that around 2 million cars have the odometer information maliciously modified each year [11].

In some instances (e.g. 2010 Ford Escape) the IC is connected directly with the RF enabled chip part of the Passive Anti-Theft System (PATS) [7]. In this case, when the on-board computer starts the authentication mechanism the IC will take over the authentication data and send it to the key transceiver. The response (identification code) from the key is received and sent back to the BCM that will process the data and take the necessary action.

The functionalities offered by the ICs had an immediate impact on the computational requirements. These vary greatly due to different type of implementations employed by the automotive manufacturers. Different types of IC implementations coexists (e.g., classical gauges with mechanical needle, hybrid implementation and full LCD) which have a great impact on the computational requirements. Several processors designed for building ICs are presented in Table I. For gauges with mechanical needle and central add on display microcontrollers that embed stepper motor controllers and support for WVGA displays are employed. These come with core speeds ranging between 100 and 200 MHz. The full LCD implementation ICs rely on multiple core system on chip(SoC) solutions with clock speeds greater than 1GHz and integrated 2D and 3D processors. One IC processor solution comes from NVIDIA, the market leader in graphics processing units (GPU). Its SoC solutions for mobile devices TEGRA 3 are being used by several automotive manufacturers including Audi and Tesla.

III. Risk analysis

Having a crisper image of IC functionalities, interconnectivity and related embedded platforms we now proceed to a more comprehensive risk analysis.

A. Reported attacks

An IC flooding attack on a Scania truck using CAN diagnostic messages is presented in [12]. The IC acts as a gateway between the Infotainment CAN and the rest of car. The firewall implementations reject CAN frames that are not described in the requirements but diagnostic CAN messages are used to flood the CAN network. This makes some functionalities unavailable (IC filled with warnings) and prevents heart beat messages from being sent (due lower priority) leading to the malfunction of all the IC indicators.

Koscher et al.[5] were able to display arbitrary messages on the IC, falsify the speedometer and fuel level information and adjust the display brightness. These were performed as replay attacks based on packet sniffing and fuzzing. DoS attacks have also been performed by disabling communication from the ECM (a case in which the reported speed drops to 0 MPH) and by disabling communication from the BCM (a case in which the speed freezes to the last received value). As part of another extensive security analysis Miller and Valasek [6] presented CAN network impersonation attacks used to falsify the status of door locks, speedometer, tachometer, odometer and on board navigation. In this case, forged frames had to be sent more often than the valid frames to obtain the desired effect. Attacks based on diagnostic services have been also employed to falsify the reported fuel level.

A Mini Cooper S IC attack that uses the speedometer and tachometer to display a clock by using spoofed CAN messages sent by an impersonating microcontroller is presented in [13]. The identification of IC CAN frames was also done by packet sniffing and fuzzing the data from normal CAN traffic until the signals carrying the desired information was identified. Other replay attacks based on packet sniffing and fuzzing are presented by Hoder et al. which manage to falsify the speedometer and odometer information. They also provide hardware schematics and corresponding software for building the tool needed for mounting the attacks [14].

B. Risk analysis

In order to identify the most critical information displayed on the IC a risk assessment of the functionalities is made taking into consideration the impact and difficulty of the attack. Our risk assessment is close to the analysis employed in [15], [16] and [17]. That is, the impact of an attack is evaluated based on the following three terms along the following ranking proposed: i) *safety*, the impact of an attack on the physical integrity of the driver, passengers of the car and on other traffic participants (0 - no injury, 1 - light injury, 2 - severe, 3- life threatening, 4- fatal), ii) *financial*, the cost of the damage (0 - none, 1 - 10$, 2 - 100$, 3 - 1000$, 4 - 10000$), iii) *operational*, the impact on the functional integrity of the vehicle and the consequences over other vehicles in traffic (0-no operational impact, 1 - impacts operation but is indiscernible to driver and causes little performance concerns, 2 - discernible to driver but insignificant to other vehicles, 3 - noticeable impact both for the driver and other vehicles, 4 - significant impact for driver and other vehicles in traffic).

With small refinements, our ranking for the impact is similar to the one proposed by [15]. Since the IC attacks do not seem to pose a privacy threat, the privacy term is excluded from the current risk analysis. It is debatable if the values for these three terms (safety, privacy and operational) can be merged into a single term since they do quantify distinct objects. However, for a uniform analysis this seems the best we can do. For each of these terms we use a fixed coefficient to quantify its overall impact. We consider safety the most important one followed by the financial and operational aspects and thus set these coefficients to: $\alpha_{Sf} = 8$, $\alpha_{Fin} = 4$ and $\alpha_{Op} = 2$. These values are similar to the ones from the risk analysis that we performed in [17] and our intention is to give safety the highest level of importance. Consequently, we compute the impact as following: $\mathbb{I} = \alpha_{Sf} I_{Sf} + \alpha_{Fin} I_{Fin} + \alpha_{Op} I_{Op}$.

Risk analysis has also to consider the difficulty to carry on an attack, i.e., the time spent to prepare and carry on the attack, the level of expertise and level of insider knowledge required. We considered that all of the previous attacks are based on the same case of a compromised ECU or malicious OBD device that is used to access the CAN network and send forged frames. The risk of an attack is defined as the product of attack impact and the attack difficulty β_{DIF}: $\mathbb{R} =$

Table I
CHARACTERISTICS OF SOME COMMONLY USED DEVICES FOR IC MODULES

class	CPU model and characteristics	Communication interfaces and capabilities
low	*NXP Qorivva MPC56xxS family: MPC5645S*, 32bit e200z4d core, 125 MHz, 64KB RAM, 2MB FLASH, 64KB EEPROM	LIN: 4 ch.; CAN: 3 ch., 2x parallel data interface (PDI) WVGA, 6 x Stepper Motor Controller, Sound Generator Module, Secure Digital HW Controller
middle	*Renesas RH850/D1M family*, 32bit RH850G3M core, 240 MHz, 512KB RAM, 5MB Flash, 64KB EEPROM	LIN: 4 ch., CAN (CANFD): 3 ch., Ethernet AVB MAC (ETNB), Intelligent Stepper Motor Driver: 6 ch., Media Local Bus (MLBB), Intelligent Cryptographic Unit (ICU-S2)
	Cypress Traveo S6J3200, 32bit ARM Cortex-R5F core, 240 MHz, 512KB RAM, 2112KB Flash, 64KB EEPROM	PowerVR Series 6 G6400 (3D), Renesas graphics processor2D, CAN (CAN-FD): 3 ch., Ethernet AVB, Media Local Bus (MLB), 6 stepper motor controllers, Secure Hardware Extension(SHE)
high	*NXP i.MX 6 family: MCIMX6QP6AVT1AA*, 4x 32bit ARM Cortex-A9 cores, 1 GHz, 512KB RAM, GPU 2D Vivante GC320, GPU 2D Vivante GC355, GPU 3D Vivante GC2000+	CAN: 2 ch., Ethernet: 1 ch., MLB interface to MOST, A-HAB, ARM TrustZone, Cryptographic Acceleration and Assurance Module, NIST approved RNG, Secure RAM
	Renesas R-Car H2 SoC Family: R8A77950, 4xARM Cortex-A57, 4xARM Cortex-A53, 1xARM Cortex-R7 cores, Max. 1.6 GHz, ext. RAM, ext. Flash, ext. EEPROM	PowerVR Series6XT GX6650 (3D), CAN: 2 ch. (CAN-FD support), Ethernet: 1 ch., Crypto engine (AES, DES, Hash, RSA), SecureRAM
	NVIDIA Tegra 3 SoC, 32bit 4x ARM Cortex A9 cores, 1.4 Ghz MHz, 520MHz GeForce GPU, ext. RAM, ext. Flash, ext. EEPROM	Audio/Video decoders, display controller

$\mathbb{I} \times \beta_{DIF}^{-1}$. In our evaluation we used $\beta_{DIF} = 14$ similar to the work in [17] in order to have a common scale in evaluating the risk.

Table II lists the most important information displayed on the IC, furthermore for each function a potential attack is considered so the impact and the risk values are computed. For brevity, we defer all comments related to the impact of the attacks to the last column of Table II. Compared to the risks associated to BCM units that are analyzed in [17] the resulting risk level for ICs is comparable with top scores around 4.

As can be seen in Table II the highest risks are obtained when the active state of the cruise control is falsely reported, when the electric parking brakes malfunction is not reported or when a lower speed value is displayed on the IC deceiving the driver to increase the speed. This are good premises for vehicle collisions which may result in casualties besides the financial loss. Also a very high risk is obtained for the deactivation or malfunction not reported regarding active safety systems: ESP, ABS, collision warning/avoidance, blind spot detection and TPMS.

IV. SECURITY COUNTERMEASURES

We first discuss the principles behind the design of an Intrusion Detection System (IDS) for vehicular ICs then we give some experimental results achieved by combining industry standard Matlab and CANoe simulations.

A. Designing and IDS for vehicular ICs

Due to the high impact of the information displayed by the IC and its impact to the safety of all traffic participants, we advocate the integration of a host based IDS for the IC. An IDS for the IC can be easily implemented without adding new hardware on existing microcontrollers.

Specification-based anomaly detection can be used for CAN communication. In particular, the CAN matrix specification can be used to detect certain anomalies of CAN traffic. Examples include the monitoring of frame timeout, CRC/counter fault and invalid values. It is mandatory for the intrusion monitoring to include frequency checks of the periodic frames, minimum interval between periodic and event-triggered frames as well as consistency checks of signals values where interrelations exist.

The diagnostics services are used in all the life-cycle stages of an automobile and provide a lot of powerful features such as: updating the ECU software, activating/ deactivating ECU specific functions or reading/writing certain memory areas. When probing attacks are used the attacker will send invalid diagnostics request in this case the ECU will respond with responses as: incorrect length, incorrect format, sub-function not supported or incorrect conditions. This type of situations should never occur after the car is rolled off the assembly line.

Nonetheless, a model based observer can be used to estimate values and compare them to the reported values. Simplified models can be employed to identify an attack over certain values. Table III defines the notations used in the models which we discuss next and Table IV depicts the simplified models that we extracted to verify certain values reported by the IC.

The fuel warning model is correlated with the fuel level model which uses the instant fuel consumption rate provided by the IC trip computer to easily inferred the fuel level.

More complex rules are available for the Tire Pressure Monitoring System (TPMS), a system which is currently mandatory in the USA and Europe. Currently two implementations can be found on the market: indirect (which use information from the ABS to infer the status of the tire) and direct measurement systems (which use a dedicated sensor on each wheel). For the case in which the car is already equipped with a direct TPMS we advocate the usage of an indirect TPMS for validating the data received from the sensors. Indirect TPMS implementations use the rotational wheel speed which is provided by the ABS ECU. The detection mechanism of an under-inflated tire is based on the fact that the rotational speed is higher than for a normal inflated one because its diameter decreases. Two different algorithms are used for indirect TPMS implementation: an axial algorithm and a diagonal algorithm [20]. The axial algorithm cannot detect if there is an equal drop of pressure

Table II
QUANTITATIVE RISK ANALYSIS FOR ATTACKS ON SEVERAL IC FUNCTIONALITIES

IC indicator	I_{Sf}	I_{Fin}	I_{Op}	I	Risk	Comments
Adaptive Cruise Control On	4	4	4	56	**4**	turning the indicator on or off misleads the driver to assume that the vehicle keeps a safe distance from the vehicle in front
Parking brake fault	3	4	1-3	46	**3.28**	parking on a steep surface can lead to life threatening situations
Parking brake applied	3	4	1-3	46	**3.28**	critical when parking on a ramp
Speedometer	1-3	4	1-3	46	**3.28**	false speed reports may cause accidents, e.g., unaware speeding driver
ABS system fault	1-3	1-3	1-3	42	**3**	without ABS the braking distances increases and vehicle manoeuvrability is reduced in case of wheel lockup
Brake pad wear	3	3	1-3	42	**3**	increased braking distance, malfunctions of other braking system components
ESP system fault	1-3	1-3	1-3	42	**3**	disabled ESP leads to reduced vehicle manoeuvrability
Engine fault	1-3	3	1-3	42	**3**	unreported errors can lead to engine malfunction
Forward Collision Warning	3	3	1-3	42	**3**	critical when the car is not equipped with autonomous braking
Low tire pressure	3	3	1-3	42	**3**	increased fuel consumption, increased braking distance and poor vehicle control, tire blowout in case of over-inflated tire
Low brake fluid level/fault	3	3	1-3	42	**3**	unreported malfunction of a safety critical system
Pedestrian Warning	3	3	1-3	42	**3**	pedestrian warning is critical in case of distracted drivers
Traction Control disabled	1-3	1-3	1-3	42	**3**	disabled traction control unit leads to reduced vehicle manoeuvrability
Lane Departure Warning	3	3	1-3	42	**3**	lane departure warning systems reduces the road departure crashes by 30% [18]
Light bulbs failure	3	3	1-2	40	**2.85**	lights malfunction reduces the visibility of the car, brake/turn lights malfunction at high speeds increase the reaction time for other cars
Front/Rear fog lights On	3	3	1-2	40	**2.85**	disabling rear fog lights reduces the visibility of the car
Headlight Low beams On	3	3	1-2	40	**2.85**	inactive low beams reduces the visibility of the car
Blind Spot Monitor (BSM) Warning	3	3	1	38	**2.71**	critical from the safety perspective, on the US highways 1 in 25 deaths is due to lane changes and merges [19]
Airbag/belt tensioning system fault	1-4	0	1	34	**2.43**	increased risk of fatal injuries in case of accident, the airbags reduces mortality by 63%
Airbag disabled	1-4	0	0	34	**2.43**	wrong assumption regarding the airbag status can lead to life threatening situations, e.g., (airbag deployment in case of front-mounted baby carrier)
Oil pressure low	1-2	3	1-3	34	**2.43**	low oil pressure can lead to engine malfunction
Seat belt not fastened	3	1	2	32	**2.29**	increased risk of fatal injuries in case of accident, the usage of seat belts reduces the mortality by 72%
Alternator fault	1-2	2	1-3	30	**2.14**	alternator is unable to charge the battery, driverpassengers in danger when extreme conditions, e.g., snowstorm, desert, etc.
Low coolant level	1-2	3	1	30	**2.14**	can lead to engine malfunction
Engine coolant temperature	1-2	2	1-3	30	**2.14**	unreported high engine temperature may lead to engine damage or falsely reported high temperature can make the driver stop the car
Low battery charge	1-2	2	1-3	30	**2.14**	driver/passengers in danger when extreme conditions, e.g., snowstorm, desert, etc.
Fuel level	1-2	2	2	28	**2**	car runs out of fuel in extreme conditions, e.g., snowstorm, desert, etc.
Low fuel level	1-2	2	2	28	**2**	driver/passengers in danger when extreme conditions, e.g., snowstorm, desert, etc.
Open doors/trunk	2	2	1	26	**1.86**	opened door while driving represents a serious threat to car occupants
Park Assist Activated	1	2	3	22	**1.57**	minor threat
Tachometer	1	1	1-3	18	**1.28**	fuel consumption may not be optimal with manual gear shifts
Headlight High beams On	1	1	1-2	16	**1.14**	blinding other drivers may increase the risk of accident
Odometer	0	3	1	14	**1**	odometer tampering is used to increase the resale value

Table III
SUMMARY OF NOTATIONS

$FLev$	Fuel level
$ICon_{CAN}$	Instant Fuel consumption
h	Sampling period
Thr_{FLev}	Low fuel level threshold parameter
ω_1	Front left wheel angular velocity
ω_2	Front right wheel angular velocity
ω_3	Rear right wheel angular velocity
ω_4	Rear left wheel angular velocity
P_i	Pressure of tire i from direct TPMS
P_{ref}	Tire i nominal pressure
Ar	Axle ratio
V	Vehicle speed [mph]
Tr	Transmission ratio
Td	Tire diameter
a	Vehicle acceleration
V	Vehicle speed
sp_V	Cruise control setpoint value
$D_{FrontCar}$	Distance to the car in the front
min_{dist}	Minimum allowed distance
$\dot{M}_{fuel}$	Fuel mass flow rate

$\dot{Q}_{rej}$	Heat rejection energy
$\dot{Q}_{air}$	Heat lost from the motor block to ambient air
$\dot{Q}_{rad}$	Heat lost by radiator
ap_{factor}	Heat rejection gain
$\dot{M}_{air}$	Air mass flow rate
bp_{factor}	Heat rejection offset
$N_{fueling}$	Number of cylinders fuelling
N_{cyl}	Number of cylinders
$C_{coolflow}$	Coolant flow rate compensation gain
Q_{LHV}	Fuel lower heating value
h_{eng}	Engine block heat transfer coefficient
A_{eng}	Engine block area
T_{eng}	Engine coolant temperature (engine outlet point temperature)
T_{air}	Air temperature
$\dot{M}_c$	Coolant mass flow rate
C_c	Coolant specific heat
T_{eng_in}	Coolant temperature at engine inlet point
$A_{Thermostat}$	Thermostat opening coefficient

Table IV
INTRUSION DETECTION RULES FOR CERTAIN FUNCTIONALITIES

Functionality	Simplified model for detection
Fuel level	$FLev_{est}[t] = FLev_{CAN}[t-1] - h(ICon_{CAN}[t] + ICon_{CAN}[t-1])/2$, $\lvert FLev_{CAN}[t] - FLev_{est}[t]\rvert < \varepsilon_{FLev}$
Fuel warning	$FLev_{CAN}[t] < Thr_{FLev}$ and $Fuelwarning_{CAN} = ON$
TPMS	$Z_a = (\omega_1[t]/\omega_2[t]) - (\omega_4[t]/\omega_3[t])$, $Z_d = (\omega_2[t]/\omega_4[t]) - (\omega_1[t]/\omega_3[t])$,
	$\lvert Z_a\rvert < \varepsilon_{TPMS}$ or $\lvert Z_d\rvert < \varepsilon_{TPMS}$, $\lvert P_i[t] - P_{ref}\rvert/P_{ref} < 0.3, \forall i \in \{1,2,3,4\}$,
under-inflated	$Z_a < 0$ and $Z_d < 0$ - rear left, $Z_a < 0$ and $Z_d > 0$ - front right,
identification:	$Z_a > 0$ and $Z_d < 0$ - front left, $Z_a > 0$ and $Z_d > 0$ - rear right
RPM, speed, gear	$\lvert[(Ar\,V[t]\,Tr[t]336.13)/Td] - RPM[t]\rvert < \varepsilon$
Speed	$V_{est}[t] = V_{CAN}[t-1] + h(a_{CAN}[t-1] + a_{CAN}[t])/2$
	$\lvert V_{CAN}[t] - V_{est}[t]\rvert < \varepsilon_V$
Cruise control	$\lvert sp_V - V[t]\rvert < \varepsilon_{SPV}$, $D_{FrontCar}[t] > min_{dist}$
Engine coolant temperature	$\lvert T_{eng\,est} - T_{eng}\rvert < \varepsilon_{T_{eng}}$, $\dot{Q}_{eng} = \dot{Q}_{rej} - \dot{Q}_{air} - \dot{Q}_{rad}$,
	$\dot{Q}_{rej} = (ap_{factor} \times \dot{M}_{air} + bp_{factor}) \times (N_{fueling}/N_{cyl}) \times \dot{M}_{fuel} \times Q_{LHV}$,
	$\dot{Q}_{air} = h_{eng} \times A_{eng} \times (T_{eng} - T_{air})$, $\dot{Q}_{rad} = \dot{M}_c \times C_c \times (T_{eng} - T_{eng\_in})$, $\dot{M}_c = A_{Thermostat} \times C_{coolflow} \times RPM$

for the wheels located on the same axis while the diagonal algorithm cannot detect an equal drop of pressure for the

diagonal wheels. A solution is to use both algorithms and in case we have just one under-inflated tire it is possible to identify it. According to [21] a minimum of 20% - 30% pressure drop is necessary for detecting an under-inflated tire. The open problem that remains is to detect the cases when all the tires have the same pressure loss (this is not possible by using these indirect measurements).

The current vehicle speed can also be calculated based on the previous vehicle speed value and the average acceleration. The car's transmission expression [22] can be found in Table IV linking the vehicle speed, motor rotational speed and selected gear. This can be employed to identify a masquerade attack on one frame containing information on vehicle speed, RPM or active gear. The drive axle ratio parameter is specific for each vehicle model. The transmission ratio is a parameter which depends on the gear used where the correlation of gear-transmission ratio is specific for each gearbox model. More specific modifications can be detected based on these parameters.

In Figure 2 we give an overview of the structure of the proposed IDS. The system reacts to five potential indicators of bus misbehaviour to determine the presence of an intrusion: wrong counters or CRCs, incorrect range of the values, wrong dynamic variation of the values, bad timings and finally behaviour inconsistent with model based observer predictions. Actions undertaken by the IDS actions includes informative actions (alarms) and attack mitigation actions. Informative actions refer to informing the driver about a possible intrusion (through an IC notification) and/or informing the automotive maker/fleet owner when telematics systems are employed. The attack mitigation component should be responsible of changing the system state, e.g., switching to limp mode (a state which still enables the vehicle to function safely with limited functionality) or shutdown in extreme situations along with ignoring frames that are recognized as malicious.

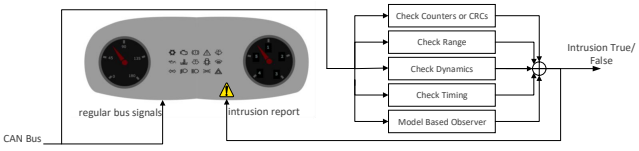


Figure 2. Intrusion detection mechanisms

B. Experimental results

As proof-of-concept experiments, we pursue the integration of a more complex model for the engine coolant temperature as presented in [23]. The engine coolant temperature model from [23] employs information available from production Engine Control Modules (ECM) to compute the engine coolant temperature. This model was proposed for the identification of various cooling system faults to provide temperature in case of coolant temperature sensor (CTS) malfunctions. The procedure was successfully validated by the authors in [23] on a production Engine Control Module (ECM).

The importance of the engine coolant temperature information comes from the fact that by decreasing the reported temperature value while the engine overheats due to certain adversarial manipulation (e.g., by increasing the RPM) may result in damage which generates significant economic loses. In contrast, by maliciously enabling the associated warning light on the IC, the driver may be forced to stop the car at the will of an adversary opening door for other threats.

The engine ECU provides the measured engine coolant temperature and it's derivative. The IDS can implement an observer for the engine coolant temperature by computing it along with its derivative. The IDS also computes the differences between the engine coolant temperature and engine temperature derivative received from the engine ECU and the computed values from the model, i.e., $\Delta_{T_{eng}}$ and $\Delta_{\dot{T}_{eng}}$. The IDS monitors if the difference between these values exceed some fixed thresholds, i.e., $\varepsilon_{T_{eng}}$ and $\varepsilon_{\dot{T}_{eng}}$.

The physical process is simulated in MATLAB Simulink in which the input signals T_{air}, $\dot{M}_{air}$, $\dot{M}_{fuel}$, $N_{fueling}$ and RPM are generated by a Simulink block and sent to the simulated process. These values are also sent to the VECTOR CANoe simulation software which is integrated with another Simulink implementation of the engine coolant temperature model providing estimated values for T_{eng} and $\dot{T}_{eng}$. The test environment is suggested in Figure 3. MATLAB Simulink[1] and VECTOR CANoe[2] are industry-standard tools for system modelling-simulation and testing-simulation of in-vehicle networks. We chose to mix between the two since MATLAB Simulink is the best choice for system modelling and we could easily deploy the engine coolant model in this environment. In contrast, VECTOR CANoe allows us to simulate the in-vehicle network and thus add forged CAN frames that fake the reports on various parameters. From a security perspective, adversarial capabilities are present inside the CANoe simulation while the computations of the IDS consists in the difference between the values reported by the Simulink model and the values received from the CANoe simulation. This difference is again computed in Matlab and we underline that this is not a limitation from a practical perspective since Matlab can be used to generate source code for specific microcontrollers. The Simulink signal generator block for T_{air}, $\dot{M}_{air}$, $\dot{M}_{fuel}$, $N_{fueling}$ and RPM is presented in Figure 4. The Simulink model which computes the engine coolant temperature and its derivative(T_{eng} and $\dot{T}_{eng}$) is presented in Figure 5.

Modelling uncertainty is considered for the following parameters: ap_{factor} (heat rejection gain), bp_{factor} (heat rejection offset) and $C_{coolflow}$. For each of them a 20%

[1]https://www.mathworks.com/products/simulink.html
[2]https://vector.com/vi_canoe_en.html

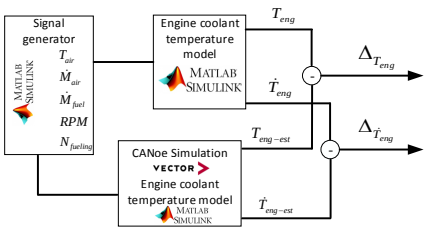


Figure 3. Test environment for engine coolant temperature model IDS

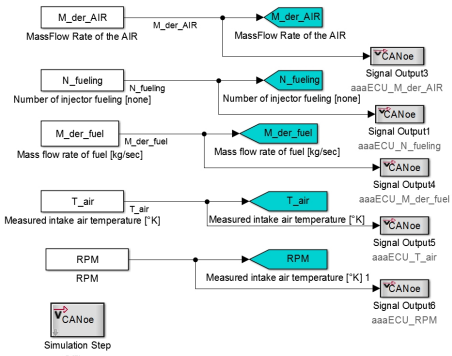


Figure 4. Simulink block diagram for the signal generator

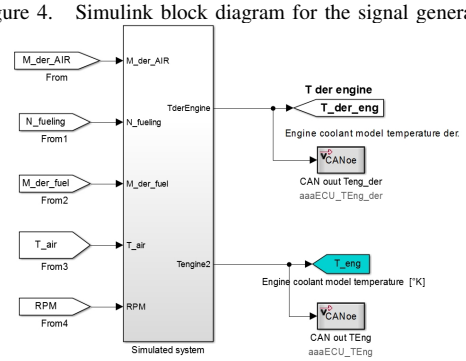
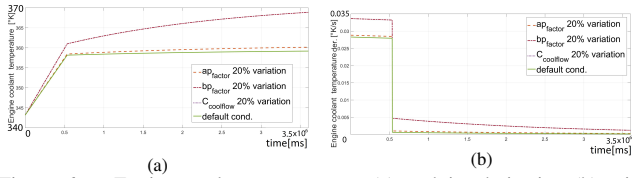
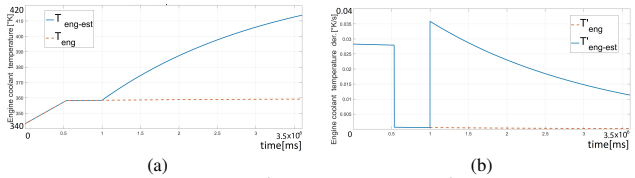


Figure 5. Simulink block diagram for the coolant temperature model



(a) (b)

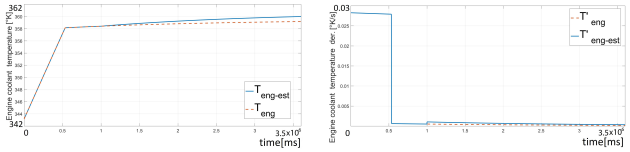
Figure 6. Engine coolant temperature (a) and its derivative (b) with modeling uncertainty



(a) (b)

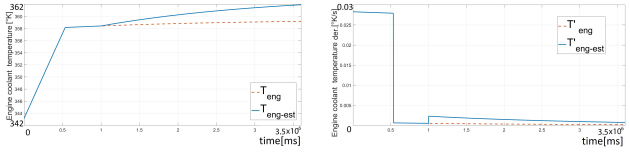
Figure 7. T_{eng} (a) and $\dot{T}_{eng}$ (b) in case of $\dot{M}_{fuel}$ signal attack

deviation from the estimated value is accepted. As can be seen in Figure 6 the bp_{factor} has the greatest impact on the engine coolant model so a proper estimation of



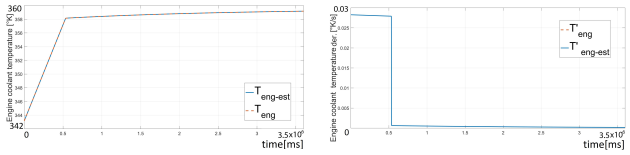
(a) (b)

Figure 8. T_{eng} (a) and $\dot{T}_{eng}$ (b) in case of $\dot{M}_{air}$ signal attack



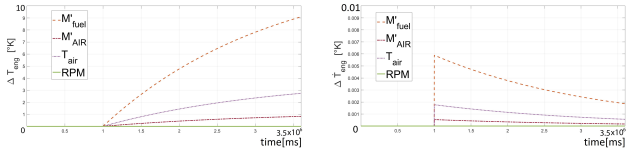
(a) (b)

Figure 9. T_{eng} (a) and $\dot{T}_{eng}$ (b) in case of T_{air} signal attack



(a) (b)

Figure 10. T_{eng} (a) and $\dot{T}_{eng}$ (b) in case of RPM signal attack



(a) (b)

Figure 11. $\Delta_{T_{eng}}$ (a) and $\Delta_{\dot{T}_{eng}}$ (b) in case of $\dot{M}_{fuel}$, $\dot{M}_{air}$, T_{air} and RPM signals attacks

this parameter is desired. Our simulation scenario considers constant values for all the parameters and inputs.

The attack scenarios that we propose consist in maliciously injecting CAN frames on the bus with the following modifications: i) a 20% increased value for $\dot{M}_{fuel}$ illustrated in Figure 7, ii) modified $\dot{M}_{air}$ illustrated in Figure 8, iii) a 4K increase for T_{air} illustrated in Figure 9, iv) a modification of RPM from 2000 to 3000 illustrated in Figure 10. All of these attacks, illustrated in Figures 7 – 10, can bypass any of the CAN frame periodicity or abnormalities checks by the IDS. They are achievable by physical access to the network and insertion of a malicious ECU node between the ECM and the CAN network or by compromising the gateway between the networks where the ECM and IC reside. False reports of coolant temperature will be easily identified for case i) and iii) due to significant differences between the received information from the CAN bus and the values computed by the model.

For the $\dot{M}_{air}$ and RPM forged signals, i.e., cases ii) and iv), the $\Delta_{T_{eng}}$ or $\Delta_{\dot{T}_{eng}}$ values are small and setting $\varepsilon_{T_{eng}}$ and $\varepsilon_{\dot{T}_{eng}}$ to identify this attack attempts will make the IDS susceptible to false positive attack detection when some of the system parameters are not properly identified. However, according to the plots in Figure 8, modifications of $\dot{M}_{air}$ causes only small variations of T_{air} and should not be of

concern. Nonetheless, other models may be used to detect individual forgeries of $\dot{M}_{air}$. For RPM, implementing the relation between RPM, speed, gear from Table IV will identify RPM forged values and this trigger an intrusion on the RPM. Figure 11 summarizes on the detection of these attacks. It can be easily seen from these plots that modified values for values for $\dot{M}_{fuel}$, T_{air} are easily identified by $\Delta_{T_{eng}}$ or $\Delta_{\dot{T}_{eng}}$ due to significant variations of the two.

V. Conclusion

Serious consequences can take place from wrong information that is sent to the driver from the instrument cluster, our extensive risk analysis for vehicular ICs tries to bring a crisper image over the impact of such security threats. While holistic approaches for securing in-vehicle communications are expected to arrive on the market, a component based approach with intrusion detection systems based on component particularities will be beneficial. This is because of the inherent security risks of complex systems where multiple manufacuters cooperate. In contrast, for a component based approach, the manufacturer has full control over the actions associated to the particular component which in turn is more independent on the security of the other subsystems. So far our proof-of-concept implementation shows that simple detection rules can be used in addition to a model-based observer for certain systems such as the TPMS or the engine coolant gauge. Our proposal for an IDS specifically designed for vehicular ICs is only a first step and there are of course numerous aspects to be considered for practical deployments which we may pursue as future work.

Acknowledgement. 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] M. Akamatsu, P. Green, and K. Bengler, "Automotive technology and human factors research: Past, present, and future," *International journal of vehicular technology*, 2013.

[2] W. Ribbens, *Understanding automotive electronics: an engineering perspective*. Butterworth-Heinemann, 2012.

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

[4] 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), IEEE Symposium on*. IEEE, 2010, pp. 447–462.

[5] 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*, 2011.

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

[7] ——, "A survey of remote automotive attack surfaces," *Black Hat USA*, 2014.

[8] A. Boudguiga, W. Klaudel, A. Boulanger, and P. Chiron, "A simple intrusion detection method for controller area network," in *Communications (ICC), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1–7.

[9] M. Marchetti, D. Stabili, A. Guido, and M. Colajanni, "Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms," in *Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*. IEEE, 2016, pp. 1–6.

[10] K.-T. Cho and K. G. Shin, "Fingerprinting electronic control units for vehicle intrusion detection," in *25th USENIX Security Symposium*, 2016.

[11] A. V. Thiemel, D.-E. M. Janke, and D.-E. B. Steurich, "Speedometer manipulationputting a stop to fraud," *ATZelektronik worldwide*, vol. 8, no. 2, pp. 16–19, 2013.

[12] A. Asvestopoulos, "Intrusion protection of in-vehicle network: study and recommendations," 2015.

[13] J. Staggs, "How to hack your mini cooper: Reverse engineering can messages on passenger automobiles," *Institute for Information Security*, 2013.

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

[15] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddle, and B. Weyl, "Security requirements for automotive on-board networks," in *Proc. of the 9th Intl. Conf. on Intelligent Transport System Telecommunications (ITST 2009)*, 2009.

[16] L. ben Othmane, R. Ranchal, R. Fernando, B. Bhargava, and E. Bodden, "Incorporating attacker capabilities in risk estimation and mitigation," *Computers & Security*, 2015.

[17] B. Groza, H.-E. Gurban, and P.-S. Murvay, "Designing security for in-vehicle networks: a body control module (bcm) centered viewpoint," in *Dependable Systems and Networks Workshop*. IEEE, 2016, pp. 176–183.

[18] J. M. Scanlon, K. D. Kusano, and H. C. Gabler, "Influence of roadway characteristics on potential safety benefits of lane departure warning and prevention systems in the us vehicle fleet," in *Transportation Research Board 95th Annual Meeting*, no. 16-1893, 2016.

[19] D. P. Racine, N. B. Cramer, and M. H. Zadeh, "Active blind spot crash avoidance system: A haptic solution to blind spot collisions," in *Haptic Audio-Visual Environments and Games (HAVE)*. IEEE, 2010, pp. 1–5.

[20] A. M. Ivanov, V. M. Prikhodko, and S. S. Shadrin, "Development of the external indirect pressure control system in pneumatic tires," *Life Sci. J*, vol. 11, pp. 336–338, 2014.

[21] D. Mika, "Tire pressure monitoring systems-evaluation of safety, cost and system resilience," *Studies in the Architecting of Resilient Systems*, p. 58, 2009.

[22] J. Lawlor and B. Hancock, *Auto Math Handbook*. HP Books, 2011.

[23] I. K. Yoo, K. Simpson, M. Bell, and S. Majkowski, "An engine coolant temperature model and application for cooling system diagnosis," SAE Technical Paper, Tech. Rep., 2000.