Potential Cyberattacks on Automated Vehicles

Article *in* IEEE Transactions on Intelligent Transportation Systems · September 2014

DOI: 10.1109/TITS.2014.2342271

2 authors:

Jonathan Petit
OnBoard Security Inc.
41 PUBLICATIONS **634** CITATIONS
SEE PROFILE

Steven E. Shladover
University of California, Berkeley
193 PUBLICATIONS **4,049** CITATIONS
SEE PROFILE

Potential Cyberattacks on Automated Vehicles

Jonathan Petit and Steven E. Shladover

***Abstract*—Vehicle automation has been one of the fundamental applications within the field of intelligent transportation systems (ITS) since the start of ITS research in the mid-1980s. For most of this time, it has been generally viewed as a futuristic concept that is not close to being ready for deployment. However, recent development of "self-driving" cars and the announcement by car manufacturers of their deployment by 2020 show that this is becoming a reality. The ITS industry has already been focusing much of its attention on the concepts of "connected vehicles" (United States) or "cooperative ITS" (Europe). These concepts are based on communication of data among vehicles (V2V) and/or between vehicles and the infrastructure (V2I/I2V) to provide the information needed to implement ITS applications. The separate threads of automated vehicles and cooperative ITS have not yet been thoroughly woven together, but this will be a necessary step in the near future because the cooperative exchange of data will provide vital inputs to improve the performance and safety of the automation systems. Thus, it is important to start thinking about the cybersecurity implications of cooperative automated vehicle systems. In this paper, we investigate the potential cyberattacks specific to automated vehicles, with their special needs and vulnerabilities. We analyze the threats on autonomous automated vehicles and cooperative automated vehicles. This analysis shows the need for considerably more redundancy than many have been expecting. We also raise awareness to generate discussion about these threats at this early stage in the development of vehicle automation systems.**

***Index Terms*—Automated vehicle, autonomous vehicle, cooperative automated vehicle, cyberattacks, security.**

I. Introduction

VEHICLE automation has been one of the fundamental applications within the field of intelligent transportation systems (ITS) since the start of ITS research in the mid-1980s. For most of this time, it has been generally viewed as a futuristic concept that is not close to being ready for deployment. A variety of research projects have advanced the enabling technologies in environmental perception and vehicle control and have produced experimental implementations to show how automation technology could be applied to road vehicles. These have led to major demonstrations in Europe, North America, and Japan [1]–[6], which have attracted intermittent attention from the general interest media and trade press. There has been ongoing academic research as well, largely out of sight of the general public [7]–[9].

Manuscript received January 29, 2014; revised June 10, 2014; accepted July 21, 2014. The Associate Editor for this paper was F. Yue.

J. Petit is with the Centre for Telematics and Information Technology, University of Twente, 7500 AE Enschede, The Netherlands (e-mail: j.petit@utwente.nl).

S. E. Shladover is with the California PATH Program Institute of Transportation Studies, University of California, Berkeley, CA 94720-1720 USA (e-mail: steve@path.berkeley.edu).

Digital Object Identifier 10.1109/TITS.2014.2342271

Public awareness of automated vehicles was increased somewhat by the Grand Challenge and Urban Challenge sponsored by the Defense Advanced Research Projects Agency in the United States. These led to the more recent work by Google on the development of a "self-driving" car, which has attracted an unprecedented level of media interest. That media interest has led to much speculation about the implications of automated driving for many societal issues (road safety, privacy, traffic flow, energy and environmental impacts, land use, economics of the vehicle industry, and cybersecurity). Most of this speculation has been ill informed, in part because the concepts of operation for automated vehicle systems have not been well defined yet. However, the interest shown by the general public has stimulated new interest in the automotive original equipment manufacturer and supplier industries, as well as in government agencies that are starting to sponsor new research on automated vehicle concepts.

The ITS industry has already been focusing much of its attention in recent years on the concepts of "connected vehicles" (United States) or "cooperative ITS" (Europe). These concepts are based on communication of data among vehicles (V2V) and/or between vehicles and the infrastructure (V2I/I2V) to provide the information needed to implement ITS applications. The vehicle industry has expressed concerns about the privacy implications and the risks of cyberattacks in these cooperative systems, particularly for the safety-critical applications involving collision warning and collision avoidance. Therefore, the ongoing research on cooperative systems includes significant efforts to identify the cyber threats and to define the strategies that need to be applied to protect against them.

The separate threads of automated vehicles and cooperative ITS have not yet been thoroughly woven together, but this will be a necessary step in the near future because the cooperative exchange of data will provide vital inputs to improve the performance and safety of the automation systems. This means that it is at least important to start thinking about the cybersecurity implications of cooperative automated vehicle systems. However, there are also potential cyber threats to the noncooperative (autonomous) automation systems that need attention. These are potentially more damaging than threats to nonautomated ITS systems because the driver may not be available to provide independent uncorrupted information or to defeat a malfunctioning system if she/he is thoroughly disengaged from the dynamic driving task.

As far as we know, this is the first investigation of the potential cyberattacks specific to automated vehicles, with their special needs and vulnerabilities. It is important to start broader thinking and discussion about these threats at this early stage in the development of vehicle automation systems so that more researchers can approach this problem from a variety of

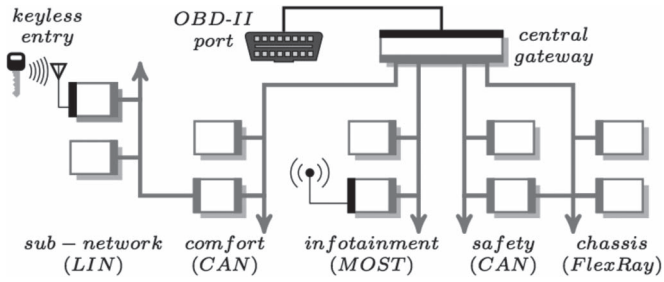

Fig. 1. Schematic of a typical in-vehicle network architecture of a modern automobile [12].

perspectives. Comprehensive protection of vehicle automation systems will require the participation of a wide range of researchers who can anticipate the widest possible range of threats; thus, we do not claim to have identified them all in this initial treatment of the subject.

Contribution: In this paper, we address the following questions.

a) How can autonomous automated vehicles be attacked?
b) How can cooperative automated vehicles be attacked?
c) What is the difference between security and privacy mechanisms for autonomous and cooperative automated vehicles?

Organization: The remainder of this paper is organized as follows. Section II gives an overview of the related work on security threats in modern automotive systems. Then, Section III defines the relevant terms related to automation, and states the assumptions considered in this paper. Section IV defines the attacker model. In Section V, we describe the methodology used to categorize the attack surfaces. Before splitting the discussion between autonomous automated vehicles and cooperative automated vehicles, we present the cross-cutting challenges in Section VI. Then, Section VII presents and discusses the security and privacy threats to autonomous automated vehicles. Likewise, Section VIII deals with cooperative automated vehicles. Finally, Section IX concludes this paper.

II. Related Work

Security analysis of modern automotive systems is a well-researched topic. More specifically, the security of in-vehicle networks has attracted attention because vehicles were not "connected" up to now. Fig. 1 illustrates the typical in-vehicle network architecture, in which Wolf *et al.* [10] investigated the endangerment of automotive bus systems (LIN, CAN, MOST, FlexRay, and Bluetooth). They also describe some feasible attacks on the protocol layer of the representative automotive bus systems, assuming that an attacker has physical or logical access to the corresponding vehicle network. Hoppe *et al.* [11] demonstrated practical controller are network (CAN) bus attacks, where an attacker can manipulate electric window lifts, warning lights, and the airbag control system.

Koscher *et al.* [13] demonstrated that an attacker who is able to infiltrate virtually any electronic control unit (ECU) can leverage this ability to completely circumvent a broad array of safety-critical systems. They demonstrate the ability to impose hostile control over a wide range of automotive functions and completely ignore driver input, including disabling the brakes, selectively braking individual wheels on demand, and stopping the engine. However, their attack provides a limited degree of automation as it does not control steering or acceleration.

Checkoway *et al.* [14] analyzed the external attack surface of a modern automobile. They discovered that remote exploitation is feasible via a broad range of attack surfaces (including mechanics tools, CD players, Bluetooth, and cellular radio), and furthermore, that wireless communications channels allow long distance vehicle control, location tracking, in-cabin audio exfiltration and theft.

We differentiate from the aforementioned works by investigating the potential cyberattacks on automated vehicle systems. Therefore, the attacks on the in-vehicle network are still present, but consequences of successful attacks might be more critical.

III. Definitions and Assumptions

A. Definitions

Automation: The use of electronic or mechanical devices to replace human labor, in this case, to replace the human labor applied to driving a road vehicle.

Autonomous Automation: Vehicle automation based entirely on information acquired from sensors onboard the vehicle, without active communication or cooperation with other entities (other vehicles or the roadway infrastructure). In the remainder of this paper, we denote a vehicle with an autonomous automation system by "autonomous automated vehicle".

Cooperative Automation: Vehicle automation that incorporates information communicated from the roadway infrastructure or other vehicles and that may also involve active negotiation of maneuvers with other vehicles. In the remainder of this paper, we denote a vehicle with a cooperative automation system by "cooperative automated vehicle."

Dynamic Driving Task [15]: All of the real-time functions required to operate a motor vehicle in on-road traffic, excluding the selection of destinations and way points (i.e., navigation or route planning) and including without limitation:

- object and event detection, recognition, and classification;
- object and event response;
- real-time mission planning;
- steering, turning, lane keeping, and lane changing;
- acceleration and deceleration;
- enhancing conspicuity (lighting, signaling, gesturing, etc.).

Minimal Risk Condition [15]: A low-risk motor vehicle operating condition to which an automated driving system automatically resorts upon either a system failure or a failure of the human driver to respond appropriately to a request to take over the dynamic driving task. A minimal risk condition could entail automatically bringing the vehicle to a stop, preferably outside of an active lane of traffic (assuming availability).

Conditional Automation [15]: The part-time and driving mode-dependent performance by an automated driving system of all aspects of the dynamic driving task with the expectation that a human driver will take over the dynamic driving task

when the automated driving system reaches the limits of its driving mode-dependent capability.

High Automation [15]: The part-time, driving mode-dependent, or geographically restricted performance by an automated driving system of all aspects of the dynamic driving task, including the ability to automatically bring the motor vehicle into a minimal risk condition when it reaches the limits of its driving mode-dependent capability, if the human driver fails to resume the dynamic driving task when prompted.

Full Automation [15]: The unconditional full-time performance by an automated driving system of all aspects of the dynamic driving task under all roadway and environmental conditions that can be managed by a human driver.

B. Assumptions

The focus of attention for this paper is on systems that provide a high enough level of automation of the dynamic driving task that the driver is no longer required to monitor the driving environment for external threats. This means that the driver's attention is likely to be focused on other subjects while the vehicle is being driven, so that some significant time (at least multiple seconds) is likely to pass before the driver is able to re-engage to take any corrective actions that may be needed. The driver can therefore not be assumed to be available all the time as the ultimate fallback to ensure safety, in contrast to the assumptions underlying the ISO 26262 functional safety standards, which assume that the driver is indeed the final guardian of safety. It is also assumed that the driver is not required to have any special training or licensing to operate an automated vehicle, so the driver behavior should be assumed to be typical of current drivers.

Within the SAE J3016 definitions of driving automation [15], this means that our focus is on the three highest levels of automation: conditional automation, high automation, and full automation, as aforementioned in Section III-A.

For the ITS systems that have been considered in previous studies of cyberattack hazards, the driver of the vehicle is always assumed to be thoroughly engaged in the driving task and paying attention to hazards in the driving environment. However, as we work up the scale of levels of automation considered here, this is clearly not necessarily the case anymore. With conditional automation systems, the driver is expected to be able to resume control of the vehicle motions within a few seconds of an adverse event, but quite a lot can happen in those few seconds (while traveling a distance of up to 100 m). With high and full automation systems, the vehicle automation system is required to bring the vehicle to a safe ("minimal risk") state even if the driver takes no action, placing a much higher burden on the designer of the system to manage any consequences of a cyberattack without compromising safety.

A cyberattack may compromise some of the sources of information that an automated vehicle uses to determine its location and plan its trajectory, while leaving other sources unaffected. Under these conditions, the data fusion software on the vehicle can play an important role in determining the true state of the vehicle and its surroundings by combining the data received from all sources. The ability of the data fusion software to successfully identify and compensate for the attack depends on the quantity and quality of the other (uncorrupted) information that remains available. At this basic level, there is no fundamental difference between data received from sensors on the subject vehicle and data communicated from other vehicles or the infrastructure, but the communicated data from the cooperative systems can represent additional data sources to augment the on-board sensor data. Indeed, cooperative adjacent vehicles and infrastructure elements (sensors) may be able to corroborate or refute observations by a vehicle that is under attack, providing independent means of verifying potentially suspect information associated with an attack. The broader the range of data sources available, the greater will be the opportunity to use data fusion to determine the true state of the vehicle and its neighborhood from the sources that remain uncorrupted.

The threats are separately analyzed for autonomous and cooperative automation systems. The autonomous systems do not include communications to support their control functions; thus, the attacks based on communications from external sources do not apply as directly to them (although they could potentially be attacked through their infotainment systems, such as any other vehicle). The cooperative systems could be subjected to the same such as the autonomous systems, in addition to another set of attacks through their communication channels. The addition of communication and cooperation opens them up to a wider range of attacks, but at the same time, the communications and cooperative data provide them with additional sources of information that can be used to identify attacks and to acquire independent information to use to compensate for an attack.

IV. Attacker Model

Here, we define the types of attackers that are likely to be present in an automated vehicle system. We follow a similar classification as [16], [17].

Internal Versus External: The internal attacker is an authenticated member of the network that can communicate with other members. The external attacker is considered by the network members as an intruder and, hence, is limited in the diversity of attacks. Nevertheless, she/he can eavesdrop on the communication.

Malicious Versus Rational: A malicious attacker seeks no personal benefits from the attacks, and aims to harm the members or the functionality of the network. Hence, she/he may employ any means disregarding corresponding costs and consequences. On the contrary, a rational attacker seeks personal profit and, hence, is more predictable in terms of attack means and attack target.

Active Versus Passive: An active attacker can generate packets or signals to perform the attack, whereas a passive attacker only eavesdrops on the communication channel (i.e., wireless or in-vehicle wired network).

Local Versus Extended: An attacker can be limited in scope, even if she/he controls several entities (vehicles or base stations), which make him/her local. An extended attacker controls several entities that are scattered across the network, thus extending his/her scope.

Intentional Versus Unintentional: An intentional attacker generates attacks on purpose, whereas an unintentional attack is a cyber incident that could be generated by faulty sensors or equipments.

In this paper, we consider all types of attackers except *unintentional* because its feasibility is difficult to assess as dependent on the sensor's quality. We also assume that an attacker can have access to his/her victim's vehicle (including in-vehicle network).

V. Methodology

To foster discussions of the security and privacy issues for automated vehicles, we first list the attack surfaces (i.e., the entry point of the attack) for autonomous automated vehicles, and cooperative automated vehicles. For each attack we define the following criteria:

a) *Means*: Describes the attack performed on the attack surface.
b) *Feasibility of the attack (FA)*: Describes the level of knowledge needed to perform the attack. The feasibility of an attack represents also the technical expertise required to launch such an attack. Some attacks might require high technical expertise with the technology or hardware that makes the attack less feasible. For example, an attacker that has the ability to extract program code and secret keys of an on-board unit (OBU) or Roadside Unit (RSU) by launching physical attacks requires high technical expertise. On the other hand, the availability of (affordable) off-the-shelf products can make an attack highly feasible. Therefore, the feasibility of an attack also depends on the attacker's resources. Budget, manpower and tools are three key resources, where for example, budget can be time (e.g., to learn the technology, to code software tools) or money (to buy equipment or software).
c) *Need for physical access to the targeted vehicle (PA)*: Is physical access to the targeted vehicle required to run the attack? (yes/no)
d) *Ease of detection by driver*: Can the driver detect the attack?[1] In Tables I and II, the symbol "$*$" means "*if the user looks at the display*" (considering that the display shows warning and upcoming maneuver for example). This criterion assumes a certain level of driver familiarity with the object of interest.
e) *Ease of detection by the system (EDS)*: Can the system detect the attack?
f) *Probability of attack success (PAS)*: Based on the previous criteria, we assess the probability of success of the attack. For example, a highly feasible attack (criterion b) but easily detected (criteria d or e) is unlikely to succeed.
g) *Consequence for the vehicle*: Describes the direct consequence(s) for the vehicle such as entering in minimal risk condition.
h) *Hazard created*: At a macroscopic point of view, describes the hazard created by the attack (e.g., traffic disturbance).
i) *Mitigation technique(s)*: Describes the mitigation technique(s) that can be deployed to mitigate the impact of such attack.

The criteria b, d, e, and f are using the risk levels: low/medium/high. A low feasibility means that the knowledge/equipment needed is not easily accessible and requires time to master. A low ease of detection means that the detection is difficult. For example, a driver cannot detect an attack on the wireless channel as she/he cannot physically see what is happening on this medium. The risk level is assigned according to our knowledge and its evolution will depend on the development of equipment and their accessibility.

The criterion "mitigation technique" proposes a general security technique that could be applied to prevent or mitigate the attack. We keep it generic on purpose as mitigation techniques should follow the best available technology concept.

We do not consider Tables I and II as exhaustive but aim at raising awareness of the issues of security and privacy in automated vehicles.

One could notice that our methodology is similar to the common Failure Modes and Effects Analysis (FMEA). The FMEA methodology is designed to identify potential failure modes for a product or process, to assess the risk associated with those failure modes, to rank the issues in terms of importance, and to identify and carry out corrective actions to address the most serious concerns [18]. We adapt the FMEA terminology to our context. For example, *"means"* is used instead of *"failure," "consequence for the vehicle"* instead of *"effect of the failure," "hazard created"* instead of *"severity,"* and *"FA"* instead of *"occurrence."* Attack trees are another formal methodology for analyzing the security of systems and subsystems. For example, attack trees were used in [19] to formalize attacks on V2V communication. However, in our context, the large number of attacks makes the trees too large and unwieldy. Moreover, attack trees do not specifically integrate the detection part, which is necessary to assess the probability of success of the attack.

VI. Cross-Cutting Issues

The level of automation could make the consequences of an attack more critical by reducing the ability of the driver to intervene. Indeed, recent research by General Motors (not yet published) has shown that drivers largely disengage from the driving task and monitoring of the driving environment after continuous intervals of fully automated driving ranging from 5 to 30 min, becoming almost totally dependent on the automation system. Therefore, even if the vehicle automation system is able to identify a threat that requires the system to disengage, the driver may not be capable of regaining control of the vehicle within a reasonable time interval (a few seconds, for example).

For both autonomous and cooperative automated vehicles, one of the technical challenges is the fusion of data collected from different sources. In [20] and [21], the authors present multisensor data fusion and data clustering techniques that

[1]Here, detection means that the user will detect an unexpected behavior of the system and will take corrective action(s).

TABLE I
ATTACK SURFACES IN AUTONOMOUS AUTOMATED VEHICLE

Target	Means	Feasibility of the attack	Physical access	Ease of detection by driver	Ease of detection by system	Probability of success	Direct consequence(s)	Hazard created	Mitigation technique
Infrastructure sign	change sign (fake, irrelevant)	low	n/a	high	low	low-medium	false reaction	traffic disturbance	harden infrastructure sign change; map database of sign in-vehicle; driver reporting
	alter (change speed), make it unreadable	high	n/a	high	low	low-medium	false/no reaction	traffic disturbance	harden infrastructure sign change; map database; driver reporting
	remove (e.g. stop sign)	high	n/a	high	low	low-medium	no reaction	traffic disturbance	harden infrastructure sign change; map database; driver reporting
Machine vision	blind (only source of information)	high	no	medium	high	high	degraded mode	driver disturbance	multiple cameras with different angle
	blind (other source of information available)	high	no	medium	high	high	turn off the camera	none	n/a
	fake picture/emergency brake light (only source of information)	low	no	medium	low	medium	false reaction	driver disturbance	other source of data
	fake picture/emergency brake light (other source of information available)	low	no	medium	low	medium	false reaction	driver disturbance	n/a
GPS	spoofing	high	no	low	medium	high	wrong positioning	traffic disturbance or crash hazard	authentication
	jamming	high	no	low	medium to high	high	no accurate positioning information available	need to stop vehicle unless other location info sources available	Anti-Jam GPS techniques, high-quality IMU
In-vehicle devices	inject malware	medium	yes for USB, no for others	low	medium	medium	depends on malware's capability	depends on malware's capability	Separation infotainment/safety buses; Intrusion Detection System/Anti-virus/Firewall
	head unit attack	medium	yes	high*	medium	medium	display unexpected information	driver disturbance	Protection of display of safety status information
Acoustic sensor	interference (electromagnetic, loud sound, inaudible)	medium	no	low to medium	low	low	turn off the sensor	n/a	filter; spectrum analysis
	fake crash sound	high	no	low to medium	low	low	false reaction	traffic disturbance	other source of data (e.g. radar)
	fake ultrasonic reflection	medium	no	low	low	low	false positive or false negative obstacle detection	traffic disturbance or low-speed crash	other source of data (e.g. lidar)
Radar	chaff	medium	no	medium	high	medium	degraded mode	traffic disturbance	filter; other source of data
	smart material (non reflective surface, invisible object)	low	no	medium	low	medium	no detection of surroundings	collision	other source of data
	jamming (saturation with noise)	high	no	low	high	medium	turn off radar/degraded mode	traffic disturbance	filter; other source of data
	ghost vehicle (signal repeater)	high	no	medium*	medium	medium	false detection	traffic disturbance	filter; other source of data
Lidar	jamming	high	no	low	high	medium	turn off lidar/degraded mode	loss of situation awareness by vehicle	filter; other source of data
	smart material (absorbent, reflective)	high	no	medium*	medium	medium	false detection (e.g. fake delineation)	traffic disturbance	filter; other source of data
Road	modify delineation	low	n/a	medium	low	low	false detection	traffic disturbance	driver reporting
	hack smart lane LEDs	low	n/a	low	low	low	false detection	traffic disturbance	
in-vehicle sensors	eavesdropping (tire pressure, bluetooth)	high	no	low	low	medium	privacy leak	none	in-vehicle security
	eavesdropping CAN bus	high	yes	medium	low	medium	reverse engineering	none	in-vehicle security
	inject CAN messages	medium	yes	medium	high	medium	false message from internal sensors	driver/traffic disturbance	in-vehicle security
Odometric sensors	magnetic attack	high	yes	low	low	medium	wrong position/navigation	traffic disturbance	other source of data
	thermal attack of gyroscope	medium	yes	low	low	low	wrong position/navigation	traffic disturbance	casing; other source of data
Electronic device(s)	EMP	low	no	low	high	medium	temporary to permanent damage to electronic components	disabling vehicle automation	EMP protection
Maps	Map poisoning	low	no	low	medium	medium	wrong maneuver	traffic disturbance, accident	authentication of maps server

enable data categorization. Then, in function of the category of data considered, different protection strategies are developed. Indeed, a robust data fusion system could potentially help in identifying anomalous inputs produced by a cyberattack, but this is only possible if there is enough redundancy in the sources of data, and the attack has not compromised a majority of those sources. If there are only two sources of information about a particular state of the vehicle, and one of them has been corrupted, the fusion system may not be able to tell which one is valid and which is not. However, with more than two sources it becomes easier to isolate an anomalous one (and an attack through multiple independent data sources requires a significantly higher level of sophistication on the part of the attacker). For cooperative automated vehicles, the data communicated from other vehicles or the roadside can be treated as another sensor input to the fusion system. However, the host vehicle system may be less trusting of that data than of the data obtained from its own sensors because its designer does not necessarily know that the source of the data (other vehicle or roadside system) has been adequately protected against corruption. This is particularly important for safety-critical vehicle maneuvering decisions.

VII. Security and Privacy Threats: Case of Autonomous Automated Vehicles

Here, we investigate the potential cyberattacks on autonomous automated vehicle by listing the attack surfaces and describing what attack(s) can be performed on this surface.

An autonomous automated vehicle can perceive its environment using multiple sensors. Recent implementations [22]–[25] use different combinations of components: ranging sensors (lidar, radar), GPS, and map for Stanford autonomous automated vehicle; stereo camera and laser for Oxford RobotCar; stereo cameras, 3-D lidar, radar, and GPS for AnnieWAY's autonomous automated vehicle. However, future autonomous automated vehicles may integrate more components, and thus, we consider the following attack surfaces.

- Infrastructure sign: Road sign (static or dynamic) installed by road operator or government agencies to inform drivers.
- Machine vision: Video image processing used for object detection (road, obstacles, road signs, etc.).
- GPS: Global Positioning System used for localization and positioning on the integrated map. We assume that the vehicle includes multiple GPS[2] (e.g., one GPS for navigation display and one for automation).
- In-vehicle devices: It includes hand-held devices brought by users. It can be connected to the infotainment system via Bluetooth, Wifi, Zigbee, or universal serial bus. This can represent an after-market device, a smartphone, or a tablet [26].
- Acoustic sensor: Acoustic sensor that recognizes a trained/known signal. For example, a crash sound sensor detects a collision faster than an airbag sensor [27] and, hence, can be used to trigger airbags earlier or for emergency braking. This component also considers ultrasonic systems, such as ultrasonic sonar.
- Radar: Active system that uses return of microwave radiation (radio waves) to detect objects.
- Lidar (light detection and ranging): Active system that uses return of infrared (IR) or visible light instead of radio waves to detect objects.
- Road: Material/structure on which the vehicles drive, including delineation of the road.
- In-vehicle sensors: Any on-board sensors that give information about the internal state of the vehicle (rotational speed of a wheel, tire pressure, etc.).
- Odometric sensors: Wheel encoders and inertial sensors (accelerometers, gyroscope, etc.) used for inertial-odometric navigation. The relative resistance of inertial measurement to remote attacks is one reason why military unmanned systems tend to use inertial measurement units (IMUs) as the primary navigation sensor.
- Electronic device(s): Generally speaking, the vehicle is a complex electronic device, but this could also apply to personal nomadic devices used by the vehicle occupants.
- Maps: In the case of non-real-time detection of road [28], maps are used to give longitudinal and lateral directions to the autonomous automated vehicle.

High Threats: According to Table I, the priority is to secure the high threats (see "high" in column "probability of success"), which are *camera (blind)* and *GPS spoofing/jamming*. GPS jamming is cheap to perform (around US $20), and some more expensive GPS jammers go even beyond jamming and perform GPS spoofing (medium threat in our system), where they replicate signals and provide false locations [29]. A professional car thief can continue about his/her business of stealing by using a combined GPS/GSM jammer to block the car's antitheft system from knowing and reporting where the vehicle is. Moreover, GPS jamming can be hard to detect for the system as GPS signals might be unavailable due to environmental constraints. Multiple mitigation techniques are presented in [30]: system-level countermeasures, countermeasures based on receiver antennas, receiver-based countermeasures, terminal/application-level countermeasures, and back-office countermeasures to counter GPS jamming and spoofing [31], [32].

Camera can be blinded by high-brightness IR LEDs or IR laser, which are cheap (around US $0.75/LED). Therefore, a mitigation technique for blinding by IR LED is to filter out the color. However, this filtering can be countered too. For example, the military solution is to use "wavelength-agile" lasers that can randomly change color, rendering any filtering useless [33], [34].

Medium Threats: Medium threats are electromagnetic pulse (EMP), map poisoning, radar confusion, lidar confusion, infection of in-vehicle devices, and manipulation of in-vehicle sensors.

EMP attack aims at damaging electronic devices such as onboard sensors and processors (ECU). EMPs are easy [35], [36] and cheap to create. For example, Yeh [36] created an EMP

[2]Without loss of generality, we denote any Global Navigation Satellite System by GPS.

generator for around US $300. However, we keep the feasibility as *low* because the generator is not powerful enough to shut down an entire vehicle (but enough for small electronic device such as smartphones).

An example of how maps can be poisoned has been demonstrated by Jeske [37]. In his attack, he shows how attackers can take control of navigation systems and, in the case of a wide distribution of floating car data, can actively control the traffic flow. This attack shows that the authenticity of traffic data cannot always be guaranteed. Nevertheless, autonomous automated systems often rely on maps to drive the vehicle, and thus, maps should be authenticated.

One attack on the radar is the creation of a ghost vehicle by using a digital radio frequency memory (DRFM) repeater. The DRFM digitizes the received signal and stores a coherent copy in digital memory. As needed, the signal is replicated and retransmitted. Being a coherent representation of the original signal, the transmitting radar will not be able to distinguish it from other legitimate signals it receives and processes as obstacles. Some countermeasures for radar jamming were mainly proposed for military applications. In particular, one countermeasure proposed by Lu *et al.* [38] aims at canceling the DRFM radar jamming.

The growth of vehicle connectivity with hand-held devices is increasing vehicle cyber risk. When hand-held devices are connected to the vehicles, virus and malware invade into the automotive electronics through vehicle entertainment systems or vehicle information terminals. Onishi [39] used the common vulnerability scoring system calculator to assess the cybersecurity vulnerability of in-vehicle networks. With an infection rate of 1% (virus or malware infection), the total number of fatalities and injuries becomes 4230, which is equal to 10% of all traffic fatalities in the United States nationwide per year (2008) [39]. Some protection mechanisms for in-vehicle sensors and in-vehicle network are proposed by the EVITA project.[3] Interested readers are forwarded to the EVITA deliverables.[4]

Even if the probability of success of an attack is an important indicator as it shows the likelihood to happen, the direct consequence(s) for the targeted vehicle is of high importance. Indeed, as shown in Table I, a blinding attack on a camera has a high probability of success, but if other sources of information are available (e.g., camera, radar, and lidar), the direct consequence is to turn off the camera. Therefore, the consequence for the driver and the automation is low as the vehicle can continue to adequately perform. This proves that a low or medium probability of success with a critical direct consequence (e.g., false reaction, disabling vehicle automation, and crash) should also be considered.

In the mitigation technique column, we denote "other source of data" other sensors or remote sensors (i.e., other vehicles). One can conclude from Table I that autonomous automated vehicles should always consider different sources of information (to the extent that they are available in the driving environment) to ensure an adequate level of redundancy, which permits identifying conflicting information and reduces uncertainty in the decision-making process. Using other sources of data would increase the cost of the automation system but is worthwhile as it significantly improves the decision making and, thus, the user's safety. One challenge is the data fusion to converge to the most appropriate action (see Section IV). Table I proposes other mitigation techniques such as authentication, intrusion detection system or antijam GPS, which require either changing of the equipment or a software update. It might also increase the computation overhead in the on-board system.

The limitations of autonomous automated vehicles include the limited line-of-sight and that it could not "see-through" objects/corners. For example, an autonomous automated vehicle that reaches the top of a hill could not scan the upcoming road and, thus, fully trusts its position and its map to decide the next trajectory. Hence, autonomous automated vehicles would benefit from having remote information from other vehicles as they could offer other points of view. In the next section, we investigate the attack surfaces for a cooperative automated vehicle and demonstrate the benefit of combining cooperative technology with automation technology for security and privacy purposes.

VIII. Security and Privacy Threats: Case of Cooperative Automated Vehicles

A cooperative automated vehicle uses a wireless communication technology to perform vehicle-to-X communication (V2X). Dedicated short-range communications (DSRC) or local thermal equilibrium are potential technologies for V2X, but in this paper, we are technology agnostic. One should note that considering line-of-sight communication (e.g., visible light, IR, radar as carrier) as V2X communication might reduce the threat level because of their intrinsic limited range.

In addition to the attack surfaces offered by the autonomous automation system, Table II shows the following attack surfaces (i.e., from where the attack could originate) for the cooperative automated vehicle.

- Infrastructure: The infrastructure defines the set of entities involved in the vehicular communication that are not mobile. Roadside communication units, map servers, and traffic signals are examples of infrastructure entities. These entities can broadcast messages such as roadside alert and signal phase and timing [40].
- Security system: The security system includes the infrastructure entities that manage security-related information. The Long-Term Certificate Authority, the Pseudonym Certificate Authority (PCA), and the Registration Authority (RA) are examples of certification authorities.
- Other vehicles: Any other vehicles equipped with a cooperative system and that is capable of sending messages in a comprehensible format for the receiving vehicle.
- Anywhere: This category includes attacks that can come from anywhere (infrastructure, security system, other vehicles).

One should notice that these attack surfaces are in addition to those presented in Table I. One difference is that the high threats are the ones triggering wrong reactions because of their

[3]http://www.evita-project.org

[4]http://evita-project.org/deliverables.html

TABLE II
ATTACK SURFACES IN COOPERATIVE AUTOMATED VEHICLE

Target	Means	Feasibility of the attack	Physical access	Ease of detection by driver	Ease of detection by system	Probability of success	Direct consequence(s)	Hazard created	Mitigation technique
Infrastructure (RSU)	fake WSA (RSA, SPAT)	high	no	low	low	high	wrong reaction/notification to driver	depends on nature of false message	authentication
	Map database poisoning	high	no	medium-high*	medium	medium-high	wrong decision by the system	traffic disturbance or safety hazard, depending on nature of attack	plausibility check
	DoS	high	no	low	high	medium	cannot process new message	unavailability of needed information, could be serious if denied safety-critical information	authentication; revocation
	shut down the infrastructure (physical access OR web-based)	low	no	medium*	high	medium	no information available	unavailability of needed information, could be serious if denied safety-critical information	harden physical infrastructure access
Security system (authority)	fake LTC	low	no	low	medium	low-medium	store wrong certificate	invalid message sent	authentication
	fake CRL	medium	no	low	medium	medium	store wrong certificate revocation list	ignore message from valid vehicle	authentication
	fake PC	medium	no	low	medium	medium	store wrong pseudonym certificate	invalid message sent	authentication
	refuse pseudonym distribution	high	no	low	high	medium	privacy decreases	none	misbehavior reporting
	store LTC-ID (linked to the protocol used)	low	no	low	low	low	privacy broken if authority compromised	none	CoPRA like protocol [41]
Other vehicle(s)	fake BSM	high	no	low	low	high	wrong reaction	erroneous response (spurious braking)	authentication; other source of data
	DoS	high	no	low	high	medium	cannot process new message	unavailability of needed information, could be serious if denied safety-critical information	authentication; revocation
	Map database poisoning	high	no	medium-high*	medium	medium-high	wrong reaction	traffic disturbance or safety hazard, depending on nature of attack	misbehavior detection
	fool DCC mechanisms	medium	no	low	medium	medium	generate more message to process	degrade channel condition	misbehavior detection
	remote flash firmware, reboot	low	no	low	high	low	system OFF during a period of time	no cooperative source of information	prevent remote control
	block pseudonym change	medium	no	low	medium	medium	privacy decreases	none	misbehavior detection
anywhere	attack vehicle's CAN bus through external communication links - issuing fake commands or DoS on CAN bus	low	no	low	medium	low-medium	potentially disabling vehicle or issuing unsafe movement commands	driver/traffic disturbance	misbehavior detection; secure coding
	location tracking	medium	no	low	low	medium	privacy decreases	none	pseudonym system

direct impact on the user's life. Thus, there is a closer link between probability of success and direct consequence. The other threats do not jeopardize the automation system in its whole, but mainly inhibit one source of information (i.e., the system does not consider this entity as a source of information for a defined period). Therefore, attacks that trigger false reaction are considered as the most dangerous ones because of their direct impact on the user's life and, thus, have the highest risk.

High Threats: The high threats are the *injection of fake safety messages* and *map database poisoning*.

In the first high threat, the infrastructure (RSU) or neighbor vehicle can inject fake messages (WAVE Service Advertisement, Basic Safety Message (BSM)), which generate wrong reactions (e.g., spurious braking) that can be life-threatening for the driver, passengers and surrounding vehicles.

The mitigation techniques mainly require the setup of an authentication system and a misbehavior detection system. Indeed, authenticated vehicles can send false information, which can only be detected by a misbehavior detection system. The misbehavior detection system is a software module on the OBU, whereas the authentication mechanism might require a more complex system in case of the establishment of a Public Key Infrastructure for example.

The second high threat is the map database poisoning. This attack is different from "map poisoning" of autonomous automated vehicles in the sense that the poisoning attack does not target an online server that collects floating car data, but targets the map database locally stored on the vehicle. The OBU stores the content of all messages (new point of interest, obstacles, construction site, etc.) in a so-called Local Dynamic Map (LDM in Europe) or Geographic Information System (GIS in the United States). From this local representation of the real world, misbehavior detection, in-network data aggregation, and more generally, decisions are taken. Therefore, poisoning this database will affect the overall cooperative system. Here, again, the mitigation technique is a misbehavior detection system, which performs plausibility checks before storing the data into the map database.

Medium Threats: One can notice that in comparison to autonomous automated vehicles, cooperative automated vehicles have fewer low threats but more medium threats. A Denial of Service (DoS) can cause a vehicle to not process any

new incoming message because the system is overloaded with messages to process. The consequences could be the increase of the uncertainty of information received (from sensors), but also, the denial of safety-critical information. As mitigation techniques, an authentication mechanism would identify the attacker, and a revocation process can be triggered to prevent this vehicle from misbehaving in the future. However, note that authentication and revocation mechanisms do not protect against jamming of radio communication, which is a feasible and inexpensive DoS attack, and difficult to mitigate. Similar to a DoS attack, an attacker can fool the Distributed Congestion Control (DCC) [42] mechanism by sending high Channel Busy Ratio (CBR) to his/her one-hop neighbors to degrade the channel condition and increase the number of messages to process (send or receive). Nevertheless, this attack is limited in space (one-hop) and impact as the DCC mechanism provides a minimal Quality of Service.

Attacks on the security system are mostly medium threats. A fake Long Term Certificate (LTC) or Pseudonym Certificate (PC) will generate invalid messages (i.e., invalid signatures), which will then be ignored by receivers. An OBU that stores a fake Certificate Revocation List (CRL) will reject messages from valid OBUs, which jeopardizes the cooperative system of the attacked vehicle. Indeed, this could be a serious safety problem if that leads to a failure to warn or avoid a crash. A mitigation technique is to authenticate the CRL, LTC, and PC before usage.

Cooperative systems will enable remote access to the automotive databus. For example, CarSpeak [43] enables a car to query and access sensory information captured by other cars in a manner similar to how it accesses information from its local sensors. This enables reading from remote sensors, but one should ensure that it is not possible to inject messages. Another example of remote access to the CAN bus without physical access was presented by Rouf *et al.* [44]. The authors have found a vulnerability in the data transfer mechanisms between CAN bus controllers and wireless tire pressure monitoring sensors, which allows misleading data to be injected into a vehicle's system and allows remote recording of the movement profiles of a specific vehicle. The researchers used equipment costing $1500, including radio sensors and special software, to eavesdrop on, and interfere with, two different tire pressure monitoring systems. The pressure sensors contain unique IDs, so merely eavesdropping enabled the remote identification and tracking of vehicles. Beyond this, readings could be altered and forged to cause warning lights on the dashboard to turn on, or even crash the ECU completely.

As the cooperative technology (V2X) enables the broadcast of beacons that reveal information such as position, speed and direction, it intrinsically enables short-term location tracking. To protect long-term privacy of passengers, a mitigation technique is to deploy a pseudonym management system. Hence, the vehicle will change pseudonym according to privacy policies that provide sufficient level of safety and privacy [45]. This does not impact the automation system per se, as there is no direct consequence on the automated driving task. Therefore, this threat is considered as *medium* but should nevertheless be tackled to ensure user's acceptance.

We can conclude that mitigation techniques are similar to the one used to secure V2X communications [46]–[48], but the consequences of successful attacks are different. Hence, because of these potential life-threatening consequences, the implementation of mitigation techniques would be different to ensure the new requirements. For example, security mechanisms have to be more efficient (i.e., lower communication and computation overhead). However, an automated highway system, in which all vehicles are cooperative and automated, would enable different security mechanisms. As an automated system is more predictable, it would provide a more stable network that would enable symmetric cryptography for example (which is lightweight and more efficient than the current standardized asymmetric cryptography). Platooning is another good example where a group-signature scheme could be applied.

IX. Conclusion and Future Challenges

This paper has identified some of the cybersecurity threats to automated vehicles, with estimates of the severity of these threats and potential strategies for mitigating or overcoming these threats. This is an initial exploratory study to identify the challenges that need to be confronted in the development of vehicle automation systems, and to start assigning priority to the most important of these challenges. One of the most important aspects of this paper is the parallel consideration of both autonomous and cooperative automated vehicles, indicating the parallels between the threats that they face and the strategies that can be used to manage those threats. No value judgments are made about the relative security of one or the other approach, but rather the need to consider security threats is evident for both. The additional information sources available to the cooperative automated vehicles can provide additional tools to verify vehicle status, to confirm or confront attacks, but they can also provide attackers with additional opportunities to do harm. Therefore, the vehicle must have sufficient redundancy in any input source to permit consensus in the presence of a determined attack on a single modality, particularly if that modality encompasses multiple sources of information (e.g., GPS localization and cooperative communications), and if the reaction to false information is likely to be highly disruptive. Systems should also be designed to fail gracefully in the event of coordinated attacks across multiple modalities.

The main goal of this paper is to raise awareness of the importance of the issue and to stimulate others to add their thoughts about potential cybersecurity threats to automated vehicles and the countermeasures that can be applied to overcome them.

This initial study identifies GNSS spoofing and injection of fake messages as the most dangerous attacks (i.e., most likely or most severe). In autonomous automated vehicles, global navigation satellite systems (GNSS) play a key role in positioning vehicles on an accurate map. Therefore, manipulating GNSS data could provoke erratic and inaccurate maneuvers, which could endanger passengers' lives. Hence, secure GNSS signal is mandatory. Selective availability/antispoofing module (SAASM) hardware is a solution but is both expensive and access restricted. In cooperative automated vehicles, an additional

high threat is injection of fake messages that would trigger inappropriate reaction. In addition to authentication that protects from external attackers, misbehavior detection is required to detect internal and unintentional attacks. The deployment of misbehavior detection systems requires a software update of the OBU, but also a fundamental change in the current standardized security architecture such as the ETSI reference architecture.

ACKNOWLEDGMENT

The authors would like to thank E. Fok, Z. Brooks, and the members of Stanford University's Dynamic Design Laboratory led by J. Christian Gerdes for their insightful comments and suggestions.

REFERENCES

[1] M. Williams, "PROMETHEUS-The European Research Programme for Optimising the Road Transport System in Europe," in *Proc. IEEE Colloq. Driver Inf.*, 1988, pp. 1–9.

[2] S. E. Shladover, "'AHS Demo '97 Complete Success' and 'The GM-PATH Platoon Scenario'," *Intellimotion*, vol. 6, no. 3, pp. 1–3, 1997.

[3] A. Benmimou, M. Lowson, A. Marques, G. Guistiniani, and M. Parent, "Demonstration of advanced transport applications in CityMobil project," *Transp. Res. Rec., J. Transp. Res. Board*, no. 2110, pp. 9–17, 2009.

[4] T. Robinson, E. Chan, and E. Coelingh, "Operating platoons on public motorways: An introduction to the SARTRE platooning programme," in *Proc. 17th ITS World Congr.*, 2010, pp. 1–11.

[5] Y. Suzuki *et al.*, "Development of automated platooning system based on heavy duty trucks," in *Proc. 17th ITS World Congr.*, 2010, pp. 1–11.

[6] E. van Nunen, M. Kwakkernaat, J. Ploeg, and B. D. Netten, "Cooperative Competition for Future Mobility," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 1018–1025, Sep. 2012.

[7] S. E. Shladover *et al.*, "Automated vehicle control developments in the PATH program," *IEEE Trans. Veh. Technol.*, vol. 40, no. 1, pp. 114–130, Feb. 1991.

[8] R. E. Fenton and R. J. Mayhan, "Automated highway studies at the Ohio State University-an Overview," *IEEE Trans. Veh. Technol.*, vol. 40, no. 1, pp. 100–113, Feb. 1991.

[9] E. D. Dickmanns, "Vision for ground vehicles: History and prospects," *Int. J. Veh. Auton. Syst.*, vol. 1, no. 1, pp. 1–44, 2002.

[10] M. Wolf, A. Weimerskirch, and C. Paar, "Security in Automotive Bus Systems," in *Proc. Workshop Embedded IT-Security Cars*, 2004, pp. 11–12.

[11] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks-practical examples and selected short-term counter-measures," in *Proc. Comput. Safety, Rel., Security*, 2008, pp. 235–248.

[12] F. Sagstetter *et al.*, "Security challenges in automotive hardware/software architecture design," in *Proc. Conf. DATE*, 2013, pp. 458–463.

[13] K. Koscher *et al.*, "Experimental security analysis of a modern automobile," in *IEEE Symp. Security Privacy*, May 2010, pp. 447–462.

[14] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proc. 20th USENIX SEC*, 2011, pp. 1–16.

[15] "Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems," Surface Veh. Inf. Rep. J3016, Jan. 17, 2014.

[16] A. Panchenko and L. Pimenidis, "Towards practical attacker classification for risk analysis in anonymous communication," in *Proc. 10th IFIP TC-6 TC-11 Int. Conf. CMS*, 2006, pp. 240–251.

[17] M. Raya and J.-P. Hubaux, "Securing vehicular Ad Hoc networks," *J. Comput. Security*, vol. 15, no. 1, pp. 39–68, Jan. 2007.

[18] SAE International, SAE J1739, Potential Failure Mode and Effects Analysis in Design (Design FMEA), Potential Failure Mode and Effects Analysis in Manufacturing and Assembly Processes (Process FMEA), Jan. 15, 2009.

[19] A. Aijaz *et al.*, "Attacks on inter vehicle communication systems—An analysis," in *Proc. 3rd Int. WIT*, 2006, pp. 189–194.

[20] B. Khaleghi, A. Khamis, F. O. Karray, and S. N. Razavi, "Multisensor data fusion: A review of the state-of-the-art," *Inf. Fusion*, vol. 14, no. 1, pp. 28–44, 2013.

[21] N.-E. E. Faouzi, H. Leung, and A. Kurian, "Data fusion in intelligent transportation systems: Progress and challenges—A survey," *Inf. Fusion*, vol. 12, no. 1, pp. 4–10, Special Issue on Intelligent Transportation Systems, 2011.

[22] M. Montemerlo *et al.*, "Junior: The Stanford entry in the urban challenge," *J. Field Robot.*, vol. 25, no. 9, pp. 569–597, Sep. 2008.

[23] P. Newman *et al.*, "Navigating, recognising and describing urban spaces with vision and laser," *Int. J. Robot. Res.*, vol. 28, pp. 1–28, Oct. 2009.

[24] J. Levinson *et al.*, "Towards fully autonomous driving: Systems and algorithms," in *Proc. IEEE IV Symp.*, 2011, pp. 163–168.

[25] A. Geiger *et al.*, "Team AnnieWAY's Entry to the 2011 Grand Cooperative Driving Challenge," *IEEE Trans. Intell. Transp. Syst.*, vol. 13, no. 3, pp. 1008–1017, Sep. 2012.

[26] J. Joy, A. Raghu, and J. Joy, "Architecture for secure tablet integration in automotive network," in *Proc. FISITA World Automotive Congr.*, 2013, pp. 683–692.

[27] M. Feser, D. McConnell, T. Brandmeier, and C. Lauerer, "Advanced crash discrimination using crash impact sound sensing (CISS)," SAE World Congress & Exhibition, Apr. 2006.

[28] Y. Gao, Y. Song, and Z. Yang, "A real-time drivable road detection algorithm in urban traffic environment," in *Proc. ICCVG*, 2012, pp. 387–396.

[29] Royal Academy of Engineering, Global Navigation Space Systems: Reliance and Vulnerabilities, Royal Academy of Engineering, 2011.

[30] C. Dixon, C. Hill, M. Dumville, and D. Lowe, "GNSS vulnerabilities: Testing the truth," *Coordinates Mag.*, vol. 8, no. 3, pp. 13–20, Mar. 2012.

[31] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. OHanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development portable GPS civilian spoofer," in *Proc. 21st Int. Techn. Meet. Satellite Division ION GNSS*, 2008, pp. 2314–2325.

[32] G. Hancke, "Security of embedded location systems," *Secure Smart Embedded Devices, Platforms and Applications*, pp. 267–286, 2014.

[33] M. Naimark, How to ZAP a camera: Using lasers to temporarily neutralize camera sensors, [Online; accessed 27-January-2014], 2002. [Online]. Available: http://www.naimark.net/projects/zap/howto.html

[34] K. N. Truong, S. N. Patel, J. W. Summet, and G. D. Abowd, "Preventing camera recording by designing a capture-resistant environment," in *Proc. 7th Int. Conf. UbiComp*, 2005, pp. 73–86.

[35] E. Aerospace, High-Power Compact Microwave Source for Vehicle Immobilization, Nov. 2011, [Online; accessed 27-January-2014]. [Online]. Available: https://www.ncjrs.gov/pdffiles1/nij/grants/236756.pdf

[36] D. Yeh, Electromagnetic pulse generator, [Online; accessed 27-January-2014]. [Online]. Available: http://72.52.208.92/~gbpprorg/mil/herf/FinalReportDavidYeh.pdf

[37] T. Jeske, "Floating car data from smartphones: What Google and Waze know about you and how hackers can control traffic," in *Proc. BlackHat Europe*, Mar. 2013, pp. 1–12.

[38] G. Lu, D. Zeng, and B. Tang, "Anti-jamming filtering for DRFM repeat jammer based on stretch processing," in *Proc. 2nd ICSPS*, 2010, vol. 1, pp. 78–82.

[39] H. Onishi, "Paradigm change of vehicle cyber security," in *Proc. 4th Int. Conf. CYCON*, 2012, pp. 1–11.

[40] "Dedicated short range communications (DSRC) message set dictionary," Warrendale, PA, USA, SAE J2735, Draft Rev. 35, 2014, to be published.

[41] N. Bißmeyer, J. Petit, and K. M. Bayarou, "CoPRA: Conditional pseudonym resolution algorithm in VANETs," in *Proc. 10th IFIP/IEEE Annu. Conf. WONS*, 2013, pp. 9–16.

[42] *Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part*, ETSI TS 102 687 V1.1.1, 2011, ETSI TC ITS.

[43] S. Kumar *et al.*, "CarSpeak: A content-centric network for autonomous driving," *SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 4, pp. 259–270, Aug. 2012.

[44] I. Rouf *et al.*, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proc. 19th USENIX Conf. Security*, 2010, pp. 1–16.

[45] S. Lefèvre, J. Petit, R. Bajcsy, C. Laugier, and F. Kargl, "Impact of V2X privacy strategies on intersection collision avoidance systems," in *Proc. 5th IEEE VNC*, 2013, pp. 71–78.

[46] *Intelligent Transport Systems (ITS); Security; Security Header and Certificate Formats*, ETSI TS 103 097 V1.1.1, 2013, Standard, TC ITS.

[47] *Intelligent Transport Systems (ITS); Security; Trust and Privacy Management*, ETSI TS 102 941 V1.1.1, 2012, ETSI TC ITS.

[48] *Intelligent Transport Systems (ITS); Security; Security Services and Architecture*, ETSI TS 102 731 V1.1.1, 2010, ETSI TC ITS.

Jonathan Petit received the Ph.D. degree in networks, systems, and architecture from University of Toulouse, Toulouse, France, in 2011.

He is a Postdoctoral Fellow with the Services, Cybersecurity and Safety Group, University of Twente, Enschede, The Netherlands. He is a Technical Coordinator with the European FP7 PRESERVE project. His research interests include security and privacy, intelligent transportation system, wireless, and vehicular communication.

Steven E. Shladover received the degree in mechanical engineering, with a specialization in dynamic systems and control, from Massachusetts Institute of Technology, Cambridge, MA, USA, where he began conducting research on vehicle automation in 1973.

He is the Program Manager, Mobility, with the California PATH Program, Institute of Transportation Studies, University of California, Berkeley, CA, USA. He joined the PATH Program in 1989, after eleven years with Systems Control, Inc. and Systems Control Technology, Inc., where he led the company's efforts in transportation systems engineering and computer-aided control engineering software products. He has been active in American Society of Mechanical Engineers (ASME) as the former Chairman of the Dynamic Systems and Control Division, Society of Automotive Engineers (SAE) ITS Division, and the Transportation Research Board as the Chairman of the Committee on Intelligent Transportation Systems from 2004 to 2010 and a member of the Committee on Vehicle-Highway Automation from its founding until 2010 and Chairman since 2013. He also was the Chairman of the Advanced Vehicle Control and Safety Systems Committee of the Intelligent Transportation Society of America from its founding in 1991 until 1997.

Dr. Shladover leads the U.S. delegation to ISO/TC204/WG14, which is developing international standards for vehicle-roadway warning and control systems.