Likelihoods of Threats to Connected Vehicles

LOTFI BEN OTHMANE[1], RUCHITH FERNANDO[2], ROHIT RANCHAL[2], BHARAT BHARGAVA[2], and ERIC BODDEN[3]

[1]Fraunhofer Institute for Secure Information Technology, Germany

[2]Purdue University, USA

[3]Technische Universität Darmstadt, Germany.

Connected vehicles communicate with neighboring vehicles, road side units, personal devices, and service centers; and have their electronic control units communicate through their in-vehicle networks. This provides cyber-attackers with the opportunity to communicate with the vehicles and to stage attacks. This paper reports about a case study for estimating the likelihoods of threats for connected vehicles; it provides the results of a survey that we conducted to estimate the likelihoods of 7 threats to connected vehicles. The experts rated 6 threats as "very unlikely" and one as "almost impossible" The survey shows that attacks on connected vehicles needs to be fast (before being discovered or the attack context changes) and be staged by experts who have deep knowledge about the targets. It also shows that developing such attacks does not require long time, neither expensive equipment and tools. Thus, cyber-attacks on connected vehicles are not lab experiments anymore; they are real threats for the society.

Keywords: Risk Estimation, Connected Vehicles

1. INTRODUCTION

A motor vehicle, as depicted by Figure 1, uses a set of sensors and Electronic Control Units (ECUs) that communicate through an in-vehicle network to control the operations of the vehicle. Connected vehicles communicate with neighboring vehicles, Road Side Units (RSUs), personal devices, and Service Centers (SCs) besides using an in-vehicle network. This enables the use of several applications, such as e-Call, remote startup, fleet management, and remote firmware update.

The common assumption is that attacks on vehicles can be performed only if the attacker has physical access to inject and modify messages used by connected vehicles or to change the firmware of their ECUs; that is, the in-vehicle network is a closed network. The assumption is not valid for connected vehicles because it is possible to communicate remotely with the in-vehicle network of these vehicles. This capability (the ability to use appropriate means and opportunity required to exploit a vulnerability and cause the related threats [ben Othmane et al. 2013]) allows attackers to perform cyber-attacks. For instance, an attacker, as depicted in Figure 2, could connect to the in-vehicle network of a connected vehicle and inject messages to its in-vehicle network to disable its braking system. Thus, connected vehicles are prone to cyber-threats.

There is an extensive research on developing solutions that aim to address these threats, such as the projects OVERSEE [OVERSEE project 2014], CANAuth [Van Herrewege et al. 2011] and EVITA [EVITA project 2014]. However, there are also numerous demonstrations of the feasibility of cyber-attacks on connected vehicles [Checkoway et al. 2011; Rouf et al. 2010; Miller and Valasek 2013]. Presently, the news media are active in sharing information about the security vulnerabilities of connected vehicles, e.g., [Szczesny 2014; Hern 2014]. This implies that we need to assess the *risk*s of these cyber-threats; that is, the likelihood of exercising a particular vulnerability and the resulting consequences (aka impacts) of that event [Stoneburner et al. 2002].

Ruddle et al. [Ruddle et al. 2009] analyzed the likelihood of 10 threats to Intelligent Transport Systems (ITS). They used a set of likelihood factors (e.g., the required level of expertise to develop an attack that causes the threats) to estimate the likelihood of attacks on assets. Then, they transformed the sum of the factor scores for each threat to a rating using a Likert-like scale [Likert

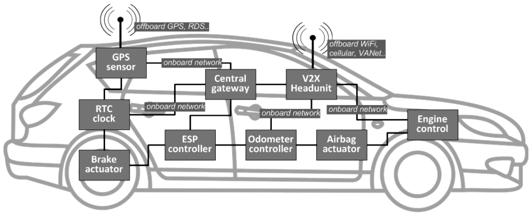


Figure 1. Example of architecture of in-vehicle network [ben Othmane et al. 2014].

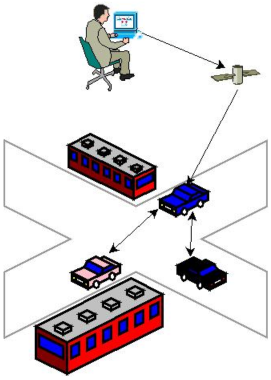


Figure 2. Example of communication paths that could be used in cyber-attacks on connected vehicles.

1932] where rates are basic, enhanced-basic, moderate, high, and beyond-high. They rated the risk likelihood of most of the threats as high and beyond-high.

This paper extends Ruddle et al. [Ruddle et al. 2009] work on assessing the security risks of connected vehicles by estimating the likelihood of 7 threats to connected vehicles using the estimates of 9 security experts (instead of one or few experts), which builds confidence and objectivity about the likelihood ratings. The main contributions are:

(1) show that the likelihood ratings of 6 out of 7 threats to connected vehicle are "very unlikely." This contrasts the current assumption that the threats to connected vehicles are lab experiments.

(2) show that connected vehicles require fast attacks (before being discovered or a change in the attack context occurs), potential attackers need to be security experts and have deep knowledge about their targets, and developing such attacks does not require long time, neither expensive equipment and tools.

The rest of the paper is organized as follows. First, we describe the state of the art of security for connected vehicles in Section 2. Then, we describe the methodology we use for estimating threat likelihood and the experiment we conducted to collect data in Section 3. Next, we discuss the results that we obtained from the experiment in Section 4 and the threats to the validity of the study in Section 5. We conclude the paper afterwards by Section 6.

2. STATE OF THE ART OF SECURITY FOR CONNECTED VEHICLES

The in-vehicle network has been proven to be insecure. For instance, Hoppe et al. [Hoppe et al. 2011] demonstrated 4 attacks that exploit the weak protection mechanisms of the in-vehicle network and were able to "maliciously" operate the window lift, warning light, airbag control system, and even the central gateway of the Controller Area Network (CAN) bus. Also, Miller and Valasek demonstrated in DEF CON 21 a set of attacks on 2 cars [Miller and Valasek 2013], showed how they reverse engineered the code of an ECU, and provided a list of keys/passwords used internally by the ECUs for cryptographic operations. They published the scripts and code they developed and the description of their attacks in [Miller and Valasek 2014a]. Miller and Valasek extended their work by analyzing the attack surfaces of 14 cases of car make, model, and fabrication year [Miller and Valasek 2014b].

Research on connected vehicle security has attracted attention in the last decade because the challenges were observed as a social barrier to the common use of connected vehicles. Most of the projects have focused on the following [ben Othmane et al. 2014]:

Table I. Remote attacks experimented on a Sedan car [Checkoway et al. 2011].

Attack	Channel	Full control	Cost
Exploit an error in the authentication program of aqLink protocol implementation and a buffer overflow vulnerability to inject malicious code to the firmware of a device connected to a vehicle.	Cellular	Yes	Medium-high
Connect through Wi-Fi to the PassThru device connected to OBD-II of a vehicle; exploit vulnerability in the device to upload a malware and communicate with other vehicles connected to PassThru devices.	Wi-Fi	Yes	Low
Use trojan horse installed on an Android-based smart phone that could be paired with the car's Bluetooth device, exploit a buffer overflow vulnerability in the car's hands-free application that uses Bluetooth protocol, and inject a malicious code in the cars′ device.	Bluetooth	Yes	Low-medium

(1) Security of communication link–protecting the confidentiality, integrity and authenticity of messages exchanged between ECUs of the same vehicle, a vehicle and communicating vehicles, a vehicle and external devices, and a vehicle and remote services.

(2) Security of devices–ensuring that the hardware and firmware of the ECUs of vehicles and on-Board Units (OBUs) are not tampered with by malicious attackers.

(3) Identity and liability–binding an entity to a specific information or event such that it is possible to prove that a specific entity (e.g., vehicle and driver) is responsible for a specific event–i.e., the entity cannot repudiate the responsibility for a specified event.

(4) Access control–enforcing rules for accessing or denying specific identified entities′ access and/or use of certain functions or data.

(5) Privacy of drivers and vehicles–enforcing the right of the driver to control the access and use of his personal data and for vehicles to control access to their identities.

There are several high level research projects that contributed to addressing these challenges, such as OVERSEE [OVERSEE project 2014], EVITA [EVITA project 2014], IntelliDrive [Intellidrive project], and SEVECOM [SeVeCom project 2014]. However, the solutions currently implemented in current vehicles provide limited efficiency in protection from malicious intended behavior–i.e., security attacks. For instance, Checkoway et al. [Checkoway et al. 2011] demonstrated a set of attacks on a connected vehicle that has e-call application–a sedan car with 100,000 to 200,000 units in USA. Table I provides a set of cyber-attacks that the authors demonstrated. These attacks demonstrate that the threat "remotely updating the firmware of an ECU" can occur. Woo et al. [Woo et al. 2014] demonstrated remotely injecting CAN command messages to the CAN of a connected vehicle such as to shutdown the engine. They used a (relay) application installed on a mobile phone that communicates using Bluetooth with an automotive diagnostic device connected to the OBDII of the target vehicle.

Ruddle et al. [Ruddle et al. 2009] analyzed the likelihood of a set of (10) threats to systems based on connected vehicles, which are: switching traffic lights green ahead of the attacker, manipulate speed limit, manipulate traffic flow, simulate traffic jam, tamper with warning messages, misuse the e-call system, Denial of Service (DoS) attack on the engine, unauthorized brake, attack active brake function, and misuse of e-toll system.[1] The authors estimated the likelihood of a set of attacks that implement the threats. They rated the risk likelihood of most of the attacks as high and very high. (They transformed the risk likelihood scores to scales as we do in this paper.)

3. STUDY METHODOLOGY

This section describes the methods we used to select a set of threats to connected vehicles, collect data, and estimate the likelihood of the selected threats.

[1] Some of the threats are also discussed in [Ruddle 2010].

Table II. Factors for estimating the ease of causing the threats.

Factor	Description
Elapsed time	Time taken to identify a vulnerability, develop and perform an attack that causes the related threat.
Specialist expertise	Level of generic knowledge about the field of connected vehicles.
Knowledge of the system	Specific expertise of various systems of connected vehicles.
Window of opportunity	Number of samples that the attacker can obtain or number of attacks without identification.
Required equipment and tools	Equipment and tools required to identify and exploit vulnerabilities related to threat t.

3.1 Method of Estimating Threat Likelihoods

This subsection describes the method we use to estimate threat likelihood. We discuss the approach for selecting the threats in Subsection 3.2.

Threat likelihood measures the expectation that potential attackers successfully perform attacks and cause the threat. However, an attacker can only perform an attack if he/she has the required capability to do so. *Attacker capability* is the ability to use the appropriate means and opportunities required to exploit a vulnerability which causes the threat [ben Othmane et al. 2014]. Attackers can use the means and opportunities they have to perform a given attack, only if they have the capabilities required to do so [ben Othmane et al. 2014].

Threat likelihood combines the ease of causing the threat and the threat occurrence frequency [ben Othmane et al. 2014]. *Ease of causing the threat* measures the difficulty attackers face in attacking the system and cause the threat. *Threat occurrence frequency* measures the expectation of the frequency of causing the threat. Equation 1 formulates the likelihood of threat t considering the threat occurrence frequency likelihood, $O(t)$, and the ease of causing the threat likelihood, $S(t)$.

$$L(t) = O(t) \times S(t) \tag{1}$$

Occurrence frequency likelihood measures the expectation of the frequency that attackers cause the threat, assuming they have required capability, means, and opportunities [ben Othmane et al. 2014]. Note that, currently, there is no data about history of attacks on connected vehicles that could be used to statistically derive occurrence frequency likelihood.

The likelihood of ease of causing a given threat measures the difficulty/complexity to have the means and opportunities to cause the threat considering the attacker capabilities [ben Othmane et al. 2014]. The means and opportunities are evaluated using the factors elapsed time, specialist expertise, knowledge of the system, window of opportunity, and required equipment and tools, which we describe in Table II. These factors are proposed by ISO 18045 [ISO (the International Organization for Standardization) and IEC(the International Electrotechnic Commission) 2008]. Other risk assessment approaches, such as OCTAVE [Alberts and Dorofee 2002] and NIST SP 800-30 [Stoneburner et al. 2002] use similar factors.

We use scores to quantify attacker capability likelihoods and likelihood factors that measure the easiness of causing the evaluated threats. The two approaches to estimate these scores are: the use of historical data and use of expert opinions. We use expert opinions as a basis for estimating attacker capability likelihood and factor scores.[2]

The score of ease of causing threat t is the sum of the scores of the n factors $\{Fl_1(t), ..., Fl_n(t)\}$ multiplied by the capability likelihood. Equation 2 formulates the ease of causing threat t considering attacker capability c_k. The ease of causing threat t is the maximum of ease of causing t considering all possible capabilities.

[2] Historical data are not currently available for the threats we study.

Table III. List of selected threats.

Threat	Description
Falsification of speedometer reading of the vehicle	An attacker may alter the speedometer reading seen by the driver, which may cause the driver to make wrong driving decisions.
Disruption of the braking system of the vehicle	An attacker may disable the breaking system while the car is in motion, or apply breaks when the driver doesn't expect it.
Disruption of the emergency response system of the vehicle (e.g., OnStar)	Some modern vehicles are equipped with emergency response systems, where the driver and passengers can contact some party to request assistance in emergency situations. An attacker may completely disable this system or falsify any information provided by the system.
Generating false check lights in the dashboard on the vehicle	Drivers depend on information displayed in the dashboard for warnings such as low tire pressure and low fuel level. An attacker may alter this information to trick the driver into driving the car until it runs out of fuel or making him/her pull over due to a false tire pressure warning.
Locking the gearstick in a fixed position	An attacker can use such an attack to render the vehicle immobile.
Sending deceptive messages to the infotainment system	Such an attack will be able to send information about a required detour to the driver and direct the driver into a trap.
Remotely updating the firmware of an ECU	Attacker may update an ECU of the vehicle with malicious firmware forcing the vehicle to misbehave.

Table IV. List of attacker capabilities.

ID	Capability
CAP-1	Attacker can physically access the OBD-II port
CAP-2	Attacker can physically access the CAN bus (e.g. connect a new ECU to the CAN bus)
CAP-3	Attacker can remotely inject messages to CAN bus
CAP-4	Attacker can spoof external GPS signals
CAP-5	Attacker can control communication between the vehicle and the Internet

$$S_t^{c_k} = (\sum_{j=1}^{j=n} Fl_j^{c_k}(t)) \times C_k(t) \tag{2}$$

3.2 Selecting Threats to Connected Vehicles

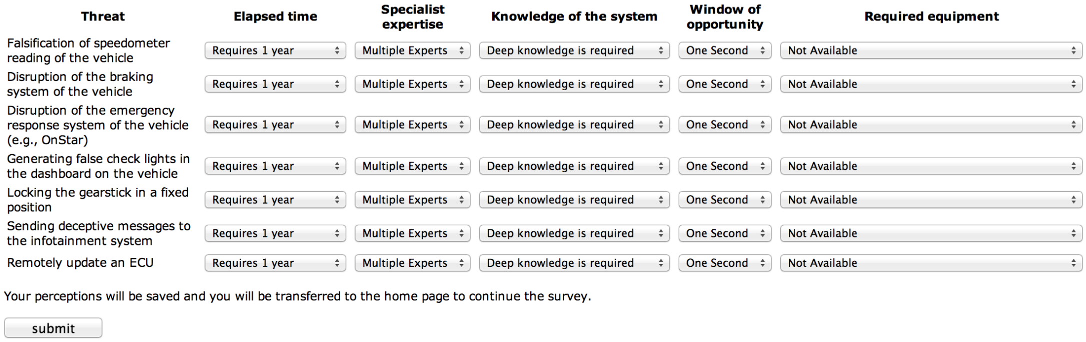
We used a standard approach to identify a set of threats specific to connected vehicles. We first enumerated vehicle components and identified the threats that affect the correct functioning of these components. Then, we chose a set of threats that we believe have high visibility. Table III describes the selected threats. These threats apply only to connected vehicles but most modern vehicles are in fact connected, e.g., offer remote locking. Attackers can cause these threats to, for example, compromise the safety of people riding the target vehicles.

The attackers need to acquire capabilities, such as remote and physical access to a vehicle's systems to be able to cause the threats. For each threat in Table III, we identified the capabilities that allow potential attackers to stage an attack. We describe these capabilities in Table IV and we provide the capabilities required for each threat in Table V.

Several attacks related to the threats of Table III have been demonstrated, e.g., in [van Ude 2014], [Miller and Valasek 2013], and [Hoppe et al. 2011]. Moreover the description of the

Table V. Relationships between selected threats to connected vehicles and attacker capabilities.

Threat	CAP-1	CAP-2	CAP-3	CAP-4	CAP-5
Falsification of speedometer reading of the vehicle	√	√	√		
Disruption of the braking system of the vehicle	√	√	√		
Disruption of the emergency response system of the vehicle (e.g., OnStar)	√	√		√	√
Generating false check lights in the dashboard on the vehicle	√	√	√		
Locking the gearstick in a fixed position	√	√	√		
Sending deceptive messages to the infotainment system	√	√		√	√
Remotely updating the firmware of an ECU			√		



Threat	Elapsed time	Specialist expertise	Knowledge of the system	Window of opportunity	Required equipment
Falsification of speedometer reading of the vehicle	Requires 1 year	Multiple Experts	Deep knowledge is required	One Second	Not Available
Disruption of the braking system of the vehicle	Requires 1 year	Multiple Experts	Deep knowledge is required	One Second	Not Available
Disruption of the emergency response system of the vehicle (e.g., OnStar)	Requires 1 year	Multiple Experts	Deep knowledge is required	One Second	Not Available
Generating false check lights in the dashboard on the vehicle	Requires 1 year	Multiple Experts	Deep knowledge is required	One Second	Not Available
Locking the gearstick in a fixed position	Requires 1 year	Multiple Experts	Deep knowledge is required	One Second	Not Available
Sending deceptive messages to the infotainment system	Requires 1 year	Multiple Experts	Deep knowledge is required	One Second	Not Available
Remotely update an ECU	Requires 1 year	Multiple Experts	Deep knowledge is required	One Second	Not Available

Your perceptions will be saved and you will be transferred to the home page to continue the survey.

Figure 3. Survey form used to assess threat likelihoods.

attacks performed by Miller and Valasek [Miller and Valasek 2013][3] and the scripts they used are available online at [Miller and Valasek 2014a].

Vehicles from different makes, models, and years of fabrication use different network architectures and protection mechanisms. However, all of them allow remote connection to their in-vehicle networks. Miller and Valasek analyzed the attack surfaces of 14 cases of vehicles with different makes, models, years of fabrication [Miller and Valasek 2014b]. The network diagrams for all the cases show that in most cases the sub-networks of each of these vehicles are able to relay messages among themselves. Considering that historically, attackers have consistently succeeding in bypassing intrusion detection systems–although progress in developing better mechanisms is constantly being made [Miller and Valasek 2014b], we believe that the inefficacy of these mechanisms will be the major weakness that attackers exploit.

3.3 Data Collection Method

We collected the attitudes/perceptions of a set of security experts about the likelihood of the set of threats for connected vehicles that we selected. We developed a Web application for collecting experts' opinions about the likelihood of the attacker capabilities and about the factors that measure the easiness to exercise the threats given the attacker capabilities. The first page of the application provides a link to a video that demonstrates DoS attack that locks the gearstick of the vehicle [van Ude 2014]. Figure 3 shows the form used by the participants to evaluate the threats.[4]

We sent invitations to participate in the study to experts who investigate security issues for

[3] Note that these attacks require physical access the OBD-II port, that is, capability CAP-1.

[4] This data collection was carried out with the Purdue University IRB authorization (Exemption #1310014174).

Table VI. Likelihood of attacker capabilities.

Capability	Mean Score	STD	Likelihood value
Attacker can physically access the OBD-II port	2.80	1.32	Unlikely
Attacker can physically access the CAN bus (e.g. connect a new ECU to the CAN bus)	2.30	1.16	Unlikely
Attacker can remotely inject messages to CAN bus	2.30	1.06	Unlikely
Attacker can spoof external GPS signals	3.10	1.10	Likely
Attacker can control communication between the vehicle and the Internet	3.10	1.29	Likely

Notes:
[1] STD stands for Standard Deviation.
[2] The mapping from score to qualitative value is: [0..1] for impossible, [1..2] for very unlikely, [2..3] for unlikely, [3..4] for likely, [4..5] for highly likely (and 5 for certain/sure).

Table VII. Mapping of threat scores to fuzzy values.

ID	Score interval	Fuzzy value
0	0..8	Almost Impossible
1	8..16	Very Unlikely
2	16..24	Unlikely
3	24..32	Likely
4	32..40	Highly Likely

connected vehicles. We received 9 full participations.

The study has two parts: assess the likelihood of attacker capabilities and assess the likelihood of success of exercising threats given attacker capabilities. The participants were asked to evaluate the likelihood that potential attackers have or be able to acquire each of the capabilities. For each capability the participants were allowed to select one of the following options "Almost Impossible," "Very Unlikely," "Likely," "Possibly," "Highly Likely," and "Certain/Sure."

Then, the participants are given the list of threats and were asked to provide their opinions about the level applicable for each of the factors that we use to estimate the likelihood of the threats (i.e., elapsed time, specialist expertise, knowledge of the system, window of opportunity, and required equipment) assuming the attacker has the required capabilities.

We used the collected data to derive statistical metrics that measure the likelihood of the 7 threats of Table III. We used the student distribution to compute the lower bound of the mean likelihood score of each threat. The student distribution is used in situations where the sample size is small [Gosset 1908]. We also used data frequency in analyzing the data that we obtained about the factors.

4. ANALYSIS OF THE STUDY RESULTS

This section describes and discusses the results, which we categorize into: attacker capabilities, likelihoods of the 7 threats, and likelihood factors.

Recall that we set the occurrence frequency likelihood to 1 because attackers who invest time and money to acquire means, opportunity, and capabilities to perform the attacks will eventually perform such attacks.

4.1 Likelihoods of Attacker Capabilities

Table VI reports the means and standard deviations of the experts' estimates of the attacker capabilities, and the likelihood of each capability derived using a mapping from score ranges to

Table VIII. Likelihood of threats to connected vehicles using likelihood value frequency.

Threat	Almost impossible	Very unlikely	Unlikely	Very unlikely or unlikely
Falsification of speedometer reading of the vehicle	11%	67%	22%	89%
Disruption of the braking system of the vehicle	22%	67%	11%	78%
Disruption of the emergency response system of the vehicle (e.g., OnStar)	22%	44%	33%	78%
Generating false check lights in the dashboard on the vehicle	22%	78%	0%	78%
Locking the gearstick in a fixed position	33%	67%	0%	67%
Sending deceptive messages to the infotainment system	11%	67%	22%	89%
Remotely updating the firmware of an ECU	67%	33%	0%	33%

Table IX. Likelihood of threats to connected vehicles using mean likelihood scores.

Threat	Mean	Low 95% CI	Likelihood rating
Falsification of speedometer reading of the vehicle	11.86	9.50	Very Unlikely
Disruption of the braking system of the vehicle	9.10	6.56	Very Unlikely
Disruption of the emergency response system of the vehicle (e.g., OnStar)	13.50	9.84	Very Unlikely
Generating false check lights in the dashboard on the vehicle	8.89	6.63	Very Unlikely
Locking the gearstick in a fixed position	9.00	6.57	Very Unlikely
Sending deceptive messages to the infotainment system	13.30	10.51	Very Unlikely
Remotely updating the firmware of an ECU	6.29	4.59	Almost impossible

Notes: The rating is derived from the lower bound of the mean scores using the CI (Confidence Interval).

qualitative values. The results show that the experts believe that potential attackers will be able to acquire the 5 capabilities with likelihoods that range from unlikely to likely. They did not perceive that it is impossible for a potential attacker to acquire any of the 5 capabilities.

4.2 Likelihood of Threats to Connected Vehicles

We used two approaches to measure the likelihood of threats to connected vehicles using: (1) likelihood value frequency and (2) mean likelihood score, where we transform the likelihood scores to qualitative values–e.g., fuzzy values [Zadeh 1978] using Table VII.[5] In general, we may understand the ratings of Table VII as follows: "almost impossible" is for threats that are still lab experiments, "very unlikely" and "unlikely" are for threats that require high expertise and knowledge, finally "likely" and "highly likely" are for threats that non-experts can cause.

In the first approach we transform the score of each expert for each threat to a qualitative value using Table VII and we compute the percentage of experts for each likelihood qualitative value and threat. We report the frequency of likelihood values for each threat in Table VIII. The table indicates that the experts estimate (67% of the experts) that the threat "remotely updating the firmware of an ECU" is "almost impossible" to occur and the other threats (i.e., "threats falsification of speedometer reading of the vehicle," "disruption of the braking system of the vehicle," "disruption of the emergency response system of the vehicle (e.g., OnStar),"

[5] The score range is divided evenly among the 5 ratings.

Table X. Elapsed Time.

Threat	Requires 1 year	Requires 1 month	Requires 1 day	Requires few minutes
Falsification of speedometer reading of the vehicle	0%	11%	78%	11%
Disruption of the braking system of the vehicle	11%	33%	44%	11%
Disruption of the emergency response system of the vehicle (e.g., OnStar)	11%	22%	33%	33%
Generating false check lights in the dashboard on the vehicle	11%	22%	56%	11%
Locking the gearstick in a fixed position	22%	0%	67%	11%
Sending deceptive messages to the infotainment system	11%	11%	33%	44%
Remotely updating the firmware of an ECU	33%	33%	33%	0%

"generating false check lights in the dashboard on the vehicle," "locking the gearstick in a fixed position," and "sending deceptive messages to the infotainment system") are "very unlikely" or "unlikely" to occur with frequency ranging from 67% to 89%.

In the second approach, we compute, for each threat the mean of the likelihood scores of the 9 experts. Table IX reports for each threat the mean score, the lower bound of the 95% confidence interval [Seltman 2014] of the mean and the likelihood rating of the mean, which is derived using Table VII. The mean scores indicate that the threat "remotely updating the firmware of an ECU" is "almost impossible" to occur and the other 6 threats are "very unlikely" to occur. These results are close to the ones obtained using the first approach in the sense that only the threat "remotely updating the firmware of an ECU" has "almost impossible" as threat likelihood.

The two approaches for measuring threat likelihood produce close results for the 7 threats, where one threat is perceived to be "almost impossible" and the other 6 threats are perceived to be "very unlikely."[6] The threats, whose likelihoods are "very unlikely," concern injecting and modifying the in-vehicle messages and the threat, whose likelihood is "almost impossible," concerns changing the code of ECUs. These results suggest that the experts perceive that it is more difficult to change the code of ECUs than to inject messages.

If we are on the conservative side, we may use the low bound of the 95% confidence interval for the mean likelihood instead of the sample mean likelihood (Recall that the mean is commonly used as the expected value, which we use here.) for rating the threats–using Table IX. In this case, 3 threats out of the 7 have the "very unlikely" likelihood rating; they are "falsification of speedometer reading of the vehicle," "disruption of the emergency response system of the vehicle (e.g., OnStar)," and "sending deceptive messages to the infotainment system." The other 4 threats have the rating,"almost impossible." In our opinion, the 4 threats that are rated "almost impossible" are strongly related to safety mechanisms and the experts may have expected that the vehicles have protection mechanisms to mitigate these threats–or were conservative in rating this category of threats.

4.3 Estimation of the Likelihood Factor' Scores

This section reports the results of estimating the scores of the factors used in computing the threat likelihoods and analyses the results.

Elapsed time. Table X reports the frequency of the scales of the time required to develop an attack for each threat in the experts' estimation. It indicates that the experts estimate that a potential attacker needs only one day or more to develop an attack for 6 of the threats and even few

[6] The threats likelihoods of the 6 threats using the first approach are unlikely and using the second approach are unlikely or very unlikely.

Table XI. Required equipment.

Threat	Not Available	Only for Experts	Expensive- e.g., 10000	Cheap equipment or script
Falsification of speedometer reading of the vehicle	0%	22%	22%	56%
Disruption of the braking system of the vehicle	11%	22%	11%	56%
Disruption of the emergency response system of the vehicle (e.g., OnStar)	11%	22%	11%	56%
Generating false check lights in the dashboard on the vehicle	11%	22%	11%	56%
Locking the gearstick in a fixed position	11%	22%	0%	67%
Sending deceptive messages to the infotainment system	0%	22%	0%	78%
Remotely updating the firmware of an ECU	22%	33%	11%	33%

Table XII. Specialist expertise.

Threat	Multiple Experts	Expert	Professional	Layman
Falsification of speedometer reading of the vehicle	0%	44%	33%	22%
Disruption of the braking system of the vehicle	11%	56%	33%	0%
Disruption of the emergency response system of the vehicle (e.g., OnStar)	11%	33%	33%	22%
Generating false check lights in the dashboard on the vehicle	11%	56%	33%	0%
Locking the gearstick in a fixed position	33%	33%	33%	0%
Sending deceptive messages to the infotainment system	11%	67%	0%	22%
Remotely updating the firmware of an ECU	56%	44%	0%	0%

minutes for one of the threats (4 experts estimate that a potential attacker needs few minutes to develop an attack that leads to sending deceptive messages to the infotainment system). We believe that the ease of developing attacks is mainly attributed to the wide availability of information, attack tools, and tutorials on the Internet that could be exploited to develop attacks on connected vehicles.

Required equipment. Table XI reports the frequency of the scales of availability of equipment and tools that could be used to cause each threat in the experts' estimation. It indicates that most of the experts estimate that the equipment and tools required to attack connected vehicles are cheap for 6 of the 7 threats. It also indicates that the experts disagree about the difficulty of obtaining the equipment and tools for the threat "remotely updating the firmware of an ECU"–two of the experts believe that the equipment and scripts to carry on such threat are not available.

Specialist expertise. Table XII reports the frequency of the scales of attackers' level of expertise on security attacks required for each threat in the experts' estimation. It indicates that, in general, the experts estimate that performing attacks that cause the 7 threats requires high level of expertise; that is, levels: multiple experts, expert, and professional. The ratio of experts who believe that cyber-attack hobbyists could cause the 7 threats, is low for all the 7 threats and believe that cyber-security hobbyists cannot trigger 3 of the 7 threats.

Knowledge of the system. Table XIII reports the frequencies of the scales of level of domain knowledge the attackers need to develop attacks that cause each of the threats in the experts' estimation. It indicates that the experts estimate that the attackers for each threat need deep or

Table XIII. Knowledge of the system.

Threat	Deep knowledge is required	Generic knowledge is required	No knowledge is required
Falsification of speedometer reading of the vehicle	67%	33%	0%
Disruption of the braking system of the vehicle	56%	44%	0%
Disruption of the emergency response system of the vehicle (e.g., OnStar)	44%	56%	0%
Generating false check lights in the dashboard on the vehicle	56%	44%	0%
Locking the gearstick in a fixed position	44%	56%	0%
Sending deceptive messages to the infotainment system	67%	33%	0%
Remotely updating the firmware of an ECU	100%	0%	0%

Table XIV. Window of opportunity.

Threat	One Day	One Year	Unlimited
Falsification of speedometer reading of the vehicle	78%	11%	11%
Disruption of the braking system of the vehicle	89%	0%	11%
Disruption of the emergency response system of the vehicle (e.g., OnStar)	89%	0%	11%
Generating false check lights in the dashboard on the vehicle	100%	0%	0%
Locking the gearstick in a fixed position	100%	0%	0%
Sending deceptive messages to the infotainment system	100%	0%	0%
Remotely updating the firmware of an ECU	100%	0%	0%

generic knowledge about connected vehicles and that a potential attacker needs deep knowledge about connected vehicles to develop an attack that causes the threat “Remote update an ECU.” We observed that the frequencies of deep knowledge and generic knowledge are close for the other 6 threats–5 experts vs. 4. Thus, we should not conclude that the results indicate either of the values for these threats.

Window of opportunity. Table XIV reports the frequencies of the scores of the time period required to cause each of the 7 threats before being discovered or the attack context changes. It indicates that, in general, the experts believe that the attackers need about one day to perform a given attack. We believe that the reason for this opinion is that vehicles are mobile, which affects attack contexts, such as the availability at a given location.

5. VALIDITY OF THE STUDY

This section argues about the validity of the study and the measures we took to control them. The classes of validity threats are: conclusion validity, internal validity, construct validity, and external validity [Wohlin et al. 2012].

Conclusion validity. This validity concerns the relationship between each experiment and the results of the related data analysis. We addressed the threats to this validity using 3 measures. First, since the sizes of the samples of both tests are limited, we used the student distribution to infer our results. The student distribution is used in situations where the sample size, drawn from a normal distribution, is small [Gosset 1908]. Second, we targeted participants who are supposed to be security experts. Third, we used two approaches to measure the likelihood of threats to connected vehicles: (1) using likelihood value frequency and (2) using the mean likelihood score.

Internal validity. This validity concerns the causal relationship between the experiments and the results of the analysis. There are 2 threats to the internal validity of the experiments. First, the questionnaire invites the participants to watch a video that shows relevant attacks, which may impact the opinions of the experts. Second, the experiment results could be affected by the quality of the questions. We addressed the second threat by testing the questionnaire before making them available online.

Construct validity. This validity concerns the relation between the experiments and the hypothesis and between the experiments and the results of the analysis. There are 2 threats to the validity of the study. The first is the difference between perception and reality in questionnaires [Likert 1932]. The second is the choice of independent variables that we used in the experiments. These variables are a set of factors for estimating the likelihood of threats and are commonly used in risk estimation methods, but their effectiveness is not verified [ben Othmane et al. 2014].

External validity. This validity concerns the condition to the generalization of the results. We analyzed 7 threats. The number is sufficient to allow generalizing the study further without high risk, given that the results are close.

We believe that threats to the validity of the study are under control. Thus, we believe that the results are valid.

6. CONCLUSION

We presented a set of threats to connected vehicles to a group of experts and asked them to estimate the likelihood of causing the threats. The experts estimated that the threat "remotely updating the firmware of an ECU" is "almost impossible" to cause by potential attackers but it is "very unlikely" that the other 6 threats are possible. We observed that experts perceive that it is more difficult to change the code of ECUs than to inject messages.

Experts estimate that potential attackers develop means to attack connected vehicles using cheap equipment and scripts rather quickly. However, some of the attacks were identified to be almost impossible for laymen to execute and to require higher levels of specialist expertise with significant system knowledge. But, the attack "remotely updating the firmware of an ECU" was deemed clearly difficult, requiring multiple experts, special equipment and deep knowledge of the system.

The results suggest that cyber-attacks on connected vehicles are practical threats. This implies that we should worry about them and consider their impacts on the society.

REFERENCES

Alberts, C. J. and Dorofee, A. 2002. *Managing Information Security Risks: The Octave Approach.* Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA.

ben Othmane, L., Ranchal, R., Fernando, R., Bhargava, B., and Bodden, E. 2014. Incorporating attacker capabilities in risk estimation and mitigation. Tech. Rep. TUD-CS-2014-0799, Center of Advanced Security Research Darmstadt, Darmstadt, Germany. Apr. http://www.tk.informatik.tu-darmstadt.de/fileadmin/user_upload/Group_CASED/Publikationen/TUD-CS-2014-0799.pdf.

ben Othmane, L., Weffers, H., and Klabbers, M. 2013. Using attacker capabilities and motivations in estimating security risk. In *Workshop on Risk Perception in IT Security and Privacy.* Newcastle, UK.

ben Othmane, L., Weffers, H., Mohamad, M. M., and Wolf, M. 2014. *Wireless Sensor Networks (WSN) For Vehicular and Space Applications: Architecture and Implementation.* Springer, Norwell, MA, Chapter A survey of security and privacy in connected vehicles. in press.

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., and Kohno, T. 2011. Comprehensive experimental analyses of automotive attack surfaces. In *Proc. of the 20th USENIX conference on Security.* Berkeley, CA, 6–6.

EVITA project. 2014. E-safety vehicle intrusion protected applications (evita). http://www.evita-project.org/. accessed on Jan. 2014.

Gosset, W. S. 1908. The probable error of a mean. *Biometrika 6,* 1 (Mar.), 1–25. (Student).

Hern, A. 2014. Self-driving cars irresistible to hackers, warns security executive. http://www.theguardian.com/technology/2014/jan/28/self-driving-cars-irresistible-hackers-security-executive. (The Guardian).

Hoppe, T., Kiltz, S., and Dittmann, J. 2011. Security threats to automotive CAN networks–practical examples and selected short-term countermeasures. *Reliability Engineering & System Safety 96,* 1, 11 – 25. Special Issue on Safecomp 2008.

Intellidrive project. Intellidrive for safety, mobility, and user fee project: Driver performance and distraction evaluation. http://www.its.umn.edu/Research/ProjectDetail.html?id=2011091. accessed on Jan. 2014.

ISO (the International Organization for Standardization) and IEC(the International Electrotechnic Commission). 2008. Information technology security techniques methodology for IT security evaluation.

Likert, R. 1932. A technique for the measurement of attitudes. *Archives of Psychology 22,* 140 (Jun.).

Miller, C. and Valasek, C. 2013. Adventures in automotive networks and control units. http://www.youtube.com/watch?v=n70hIu9lcYo. Presented at DEF CON 21 Hacking Conference. Accessed on Mar. 2014.

Miller, C. and Valasek, C. 2014a. Adventures in automotive networks and control units. http://blog.ioactive.com/2013/08/car-hacking-content.html. Accessed on March 2014.

Miller, C. and Valasek, C. 2014b. A survey of remote automotive attack surfaces. http://illmatics.com/remote attack surfaces.pdf. Presented at DEF CON 22 Hacking Conference. Accessed on Sep. 2014.

OVERSEE project. 2014. Open vehicular secure platform (oversee). https://www.oversee-project.com/. accessed on Jan. 2014.

Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., and Seskar, I. 2010. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In *Proc. of the 19th USENIX Conference on Security*. Berkeley, CA, 21–21.

Ruddle, A. 2010. Security risk analysis approach for on-board vehicle networks. In *The Fully Networked Car Workshop at the Geneva International Moto Show*. Geneva, Switzerland. http://evita-project.org/Publications/Rud10.pdf.

Ruddle, A., Ward, D., Weyl, B., Idrees, S., Roudier, Y., Friedewald, M., Leimbach, T., Fuchs, A., Grgens, S., Henniger, O., Rieke, R., Ritscher, M., Broberg, H., Apvrille, L., Pacalet, R., and Pedroza, G. 2009. Deliverable d2.3: Security requirements for automotive on-board networks based on dark-side scenarios. http://evita-project.org/Deliverables/EVITAD2.3.pdf.

Seltman, H. 2014. *Experimental design and analysis*. http://www.stat.cmu.edu/ hseltman/309/Book/Book.pdf.

SeVeCom project. 2014. Secure vehicular communication eu funded project. http://www.sevecom.org. accessed on Jan. 2014.

Stoneburner, G., Goguen, A., and Feringa, A. 2002. Risk management guide for information technology systems – recommendations of the national institute of standards and technology. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. Special Publication 800-30, accessed in May 2013.

Szczesny, J. 2014. Car-hacking: A new fear for drivers of tech-loaded vehicles. http://www.nbcnews.com/business/autos/car-hacking-new-fear-drivers-tech-loaded-vehicles-n78046. (NBC News).

Van Herrewege, A., Singelee, D., and Verbauwhede, I. 2011. Canauth-a simple, backward compatible broadcast authentication protocol for can bus. In *ECRYPT Workshop on Lightweight Cryptography 2011*.

van Ude, J. 2014. Hijacking a VW lupo via the CANbus. https://www.youtube.com/watch?v=0VZgU9ac_QI, accessed on Sep. 2013.

Wohlin, C., Runeson, P., Host, M., Ohlsson, M., Regnell, B., and Wesslen, A. 2012. *Experimentation in Software Engineering*. Springer-Verlag, Berlin Heidelberg.

Woo, S., Jo, H., and Lee, D. 2014. A practical wireless attack on the connected car and security protocol for in-vehicle can. *IEEE Transactions on Intelligent Transportation Systems PP,* 99, 1–14. To appear.

Zadeh, L. 1978. Fuzzy sets as a basis for a theory of possibility. *Fuzzy Sets and Systems 1,* 1, 3–28.

Dr Lotfi ben Othmane is currently a Scientific Researcher at Fraunhofer SIT, Germany. Previously, he worked at Lero-The Irish Software Engineering Research Center, Ireland and at the Eindhoven University of Technology, The Netherlands, as a postdoctoral researcher. He received his Ph.D. degree from Western Michigan University (WMU), USA, in 2010, M.S. degree in Computer Science from University of Sherbrooke, Canada, in 2000, and B.S degree from University of Sfax, Tunisia, in 1995. He is currently investigating the development of secure evolving software.

Dr Ruchith Fernando received his PhD in Computer Science from Purdue University. He contributed to several research projects and has six peer-reviewed publications. He received the Honorable Mention in the Research Poster Competition of 13th Annual Information Security Symposium, CERIAS. His main research interest include: user-centric identity management and security for web services.

Rohit Ranchal is a Ph. D. candidate in Computer Science at Purdue University, West Lafayette, IN. He received his M.S. in Computer Science from Purdue University in 2011 and his B.Tech. in Information Technology from Punjab Technical University, India in 2009. His research interests include monitoring, anomaly detection, policy enforcement and access control in service computing and cloud computing systems. He has received ACM Graduate Teaching Assistant Award in 2013, Raymond Boyce Graduate Teacher Award and Teaching Academy Graduate Teaching Award in 2014. He is a student member of IEEE.

Prof. Bharat Bhargava is currently a Professor of computer science at Purdue University. He received the BE degree from the Indian Institute of Science, and the MS and PhD degrees in electrical engineering from Purdue University, West Lafayette, IN. He His research involves mobile wireless networks, secure routing and dealing with malicious hosts, providing security in Service Oriented Architectures, adapting to attacks, and experimental studies. His name has been included in the Book of Great Teachers at Purdue University. Moreover, he was selected by the student chapter of ACM at Purdue University for the Best Teacher Award. He is a fellow of the IEEE.

Prof. Eric Bodden is heading the Secure Software Engineering group at Fraunhofer SIT and Technische Universitt Darmstadt. His research aims at aiding software engineers to build more secure software. This includes the design and development of novel algorithms, methods and tools for static and dynamic program analysis but also research on the proper development processes that safeguard against the introduction of software vulnerabilities. His group collaborates with various renowned research institutes and Fortune 500 companies.