Towards Comprehensive Threat Modeling for Vehicles

Mohammad Hamad*, Marcus Nolte†, Vassilis Prevelakis*
*Institute of Computer and Network Engineering, TU Braunschweig
{mhamad,prevelakis}@ida.ing.tu-bs.de
†Institute of Control Engineering, TU Braunschweig
{nolte}@ifr.ing.tu-bs.de

***Abstract*—Over the past few years, significant developments were introduced within the vehicular domain. The modern vehicle becomes a network of dozens of embedded systems which collaborate together. While these improvements have increased the efficiency of the vehicle, they have introduced new potential risks. Threat modeling has gained a central role to identifying the threats that affect different subsystems inside the vehicle. In most cases, threat modeling was implemented either for one subsystem or based on a specific perspective such as the external threat surfaces only. In this work, we tried to revise the existing threat modeling efforts in the vehicular domain. We reassembled them and extracted their main characteristics to build a comprehensive threat model. This general model could be used to identify the different threats against the vehicular domain. Furthermore, reusable attack trees could be derived from this general model.**

I. Introduction

Recently, vehicle manufacturing has changed significantly. These changes were reflected in the increased use of automotive embedded systems and the large amount of embedded software applications which were integrated within each single vehicle. the modern vehicle may contain up to 100 microcontroller-based computers, known as electronic control units (ECUs), and runs millions of lines of codes (LOC) [1], [2]. Each ECU relies on a set of sensors and actuators to serve one or more of the electrical systems or subsystems in a vehicle. Different types of communication buses (e.g. CAN, LAN, etc.) were used to interconnect the distributed ECUs inside the car. The increase of connectivity within the vehicles was a double-edged sword. On the one hand, it extended the vehicle functionalities and capabilities, but on the other hand, it opened the door for several cybersecurity threats and made the vehicle a more attractive target to adversaries [3].

The safety critical nature of the vehicle imposes the adoption of high-security measures when developing vehicular IT systems. The good understanding of the security requirements, which could be concluded from the threat modeling, is a primary step toward contriving the sufficient security countermeasures. Threat modeling helps to identify and address most of the potential threats. In fact, threats identification would likely reduce the life cycle cost of achieving security objectives when it is considered during the design process. Furthermore, threat modeling provides relevant information about the attack vectors which threaten the system. Such data could be used later as a reference during the test process to avoid the omitted threats.

Different researchers scrutinized threat modeling in the vehicular domain. However, most of the researches focused on studying the potential threats partially; by looking at threats which affect a particular sub-system, then by creating attack vectors, and by suggesting appropriate mitigation mechanisms. Practically, the lack of a general threat model, within the vehicular domain, makes threats analysis of the different subsystems a resource consuming task. On the other hand, it increases the possibility of the inconsistencies between the interacting subsystems and it causes redundancy while defining the attack vectors.

In this work, we revised the existing vehicle-related threat modeling efforts to develop a comprehensive threat model. We defined the various potential attackers' groups, nature of the attack, potential targets and security requirements of the vehicular domain. Then, we proposed an abstract model which could be used to classify all conceivable attacks against the vehicular domain. The abstract model was used as an aid to construct general attack trees [4] which illustrate the attack vectors that threaten a particular sub-system of the vehicle.

The rest of the paper is organized as follows. In section II, we reviewed the existing threat models of the vehicular domain and reassembled them. We proposed a general model, in section III, to identify the possible threats within the vehicle. In Section IV, we used our general model to identify the threats within the automated obstacle avoidance use-case. Related work was presented in section V. Finally, we presented our conclusion in section VI.

II. Threat Modeling

Threat modeling is a systematic approach for describing and classifying the security threats which affects a system. Moreover, it provides significant information that would help to safeguard the target subsystem against the attacks. Effective defense against threats requires addressing all existing security flaws in the target system and identifying threats which exploit these vulnerabilities. In addition, it demands a good comprehension about the prospective attackers, their capabilities, and their objectives. Therefore, we start exploring the threat modeling in the vehicular domain by defining the potential attackers' profiles.

A. Attacker profile

Different groups of attackers were attracted to attack the vehicles. These groups vary from the owner of the car to an expert hacker with sophisticated tools. Each one of these groups could have its own motivations:

- Falsification: An attacker (who could be the owner) may like to misrepresent the actual vehicle information such as changing the tachograph or odograph measurements to sell the car with false mileage reading.
- Illegal profit: An attacker could make a profit by stealing the vehicle or by selling the attack capability to other organization. Some attacks could be driven by a commercial competitor of the target vehicle's vendor to sabotage their product and gain the competition in the market.
- Insane fun and vandalism: revenge and vandalism could motivate some attacks as the case of a dismissed employee who sought to punish his ex-company by bricking the sold cars from this company [5].
- Research and test purposes: attacks and penetration tests could be done by security experts or test teams. The attacker, in this case, has benign motivations. They try discovering the security flaws of the different components of the vehicle before they were exploited.
- Accidental: in some circumstances, an attack could happen without any intention. such attack could occur while upgrading the existing system or reading unawares malicious data; as the case of the malfunction in vehicles GPS, climate control and front console radio systems within Toyota Lexus vehicles [6] .
- Overlap: sometimes, multiple motives could stand behind a single attack.

However, motivation alone is not enough; an attacker needs sufficient technical skills and different sets of equipment to achieve his targets. The disparity of skills, capabilities, technical equipment, and financial resources could be used as indication to classify the attackers into different groups [7]:

- Unsophisticated attackers (script kiddie): attackers with limited financial resources and insignificant knowledge about the vehicle architecture belong to this group. Such attackers lack the ability to use complicated tools. Regular thieves, owners who would like to install or replace a component within their cars, an attacker who messes up with the highway signals for gaining some reputation are all good examples of this group members
- Hacker: This group includes highly skilled experts who have the adequate tools and equipment to perform the attack. The members of this group could use their experience to get profit such as black-hat hackers. Mechanics and security researchers belong to this group.
- Organization: these organizations have multiple members of the above group who work together. The relatively massive financial support enables them to obtain the sophisticated tools and attract experts. Security research groups could be one sample of this class.

B. Attackable objects

Attackers may focus in different parts of the vehicle components such:

1) **Data:** attackers could target *stored data* in some ECUs; these data could be cryptographic private keys, digital certificates, or private vehicle and driver activities (e.g., location of vehicle, navigation destination, etc.). Or they could threaten *transferred wired/wireless data* within the vehicle. These data include: a) In-vehicle exchanged data between the different components themselves and between one component and its sensors. Spoofing the transferred data between the on-board system and the pressure sensors on the tires is an example of the vulnerability of such data [8] . b) Transferred date between the vehicle and the external world; such as V2V communication data, V2I communication data, etc.
2) **In-Vehicle Hardware**: generally, attacking the hardware infrastructure (i.e., ECUs, sensors, and OUBs) requires physical access to the target devices. Attacking In-Vehicle hardware could occur by replacing a device with a malicious one, or even installing new hardware which performs mischievously. Sometimes, the attacked hardware may not be a part of the vehicle. It could be 3rd patty devices plugged to the vehicle, such as driver's mobile phone [9]. The attacker could target to degrade the performance of the vehicle's component or even lead them to produce misleading results intentionally (e.g. Volkswagen's Emissions Scandal [10]) .
3) **Surrounding infrastructure**: Some attacks could target the surrounding environment of the vehicle. A typical example of such an attack is the modifications to the electronic road signs such as "Zombies Ahead", where an attacker figured out how to alter the text on electronic road signs warning of Zombies attack. Even such a ridiculous attack could create public safety issues for the drivers on the roadway [11].
4) **Software and framework**: the massive amount of the integrated software on each vehicle and the variety of security auditing between its different vendors make it more susceptible to attacks. the framework which controls the ECU could be a target for various attacks; some attackers could tamper with this framework of the ECU to achieve superior performance [12]. Malicious update of one application or for the framework could open the door for the attacker to vandalize the vehicle.

C. Attack requirements

1) Physical access: Some attacks are based on the physical access to the target vehicle. The direct access could happen while a vehicle is parked. Then, attackers could have a chance to attach a GPS device to track the vehicle later or target the vehicle's immobilizer and electronic locks [13]. In some circumstances, taking the car to the service station to check it could become an avenue for physical access from attackers. In such cases, an attacker

has full access to the vehicle, and he could get the benefit of using existing physical interfaces to have direct access to the internal network. On-board Diagnostic port (ODP-II) is one physical interface which was already employed in many attacks [3].

2) Remote access: Some other attacks does not require physical access to the target vehicle. Attackers could target the vehicle remotely. Such attacks take advantage of the integrated wireless features of modern cars. These features include Bluetooth, a cellular connection, wireless tire pressure monitoring, etc. The entertainment system is another point which could be remotely hacked. Playing a song laced with Malware able to emit malicious messages to the CAN bus [3].
3) Mixed access: direct access to the vehicle could be an introduction to remote attacks. Indeed, some attackers, even with rapid direct access to the vehicle, could install some devices inside the vehicle (such as a cover USB, malicious DVD, malicious component connected via OBD-II port, etc.) or outside it (communication sniffing devices). Later on, they could employ those parasitic devices to target the vehicle remotely. Attackers may use other people to install such devices, such as a valet who parks the victim's car, a mechanic at a service station [3], etc.

D. Attack effects

We could classify attacks based on their effect:

1) Limited attack: the final target of some attacks could be a single part of the vehicle. the effect of such attacks will stay bounded in the attacked ECUs and not spread anymore. The targeted system will define the jeopardy of the attack.
2) Stepping stone attack: the attack could start by compromising one component or subsystem. Later, the attacker uses this subsystem as an attack surface to plague all related subsystems. The same process could be repeated for the newly infected components. Koscher et al. [3] showed that an attacker who can control one ECU is able to attack other connected ECUs.

E. Security Requirements

1) Authentication and Integrity: providing the integrity within the vehicular systems is comprised of:

- Providing data integrity to safeguard against any modification on the data during the transaction.
- Providing message source authentication to enable the verification of the two ends of the communication.
- Providing framework and software integrity to ensure the use of only trusted code and prevent the influence of malware.
- Providing hardware integrity to prevent hardware fraud.

2) Privacy and Confidentiality: While providing authentication for the exchanged messages in the vehicular domain is vital, providing confidentiality often is less important. For example, there is no critical reason to encrypt the exchanged messages between the different ECUs inside the vehicle. Enforcing confidentiality for the exchanged data should not be mainly to prevent vehicle identification detection. The ability to identify the vehicle is feasible already by different mechanisms without the need to snoop the exchanged messages such as (identify vehicle by color, number plate, etc.) The primary goals should be preventing the leak of the driver's critical data (such as driver behavior, previous location). And to guarantee that any observer is not able to link different message, coming from the same source, efficiently. In some scenarios, confidentiality is required; for example, leaving the valuable stored information without any confidentiality protection, such as encryption, may leave the whole vehicle security at stake if an attacker is able to extract these data.

3) Availability: Availability is required especially for safety-related applications which are integrated within the vehicle. Such applications should be available even if it is under attack.

III. Abstract Model

A. Proposed model

We tried to extract the main characters of the reassembled threat model, in section III, to create an abstract model. This model could be adopted by the security experts to identify and classify the majority of threats against the vehicular systems. Such classification could reduce redundancy and inconsistencies while applying the defense techniques against the homogeneous threats. Also, it leads to defining the generic attack trees.

The proposed model shown in Fig. 1 used three layers to identify and classify the threats:

1) Target Domains: the vehicular system contains various assets (e.g. hardware, software, data, or surrounding infrastructure). Each asset may include several hidden vulnerabilities. A motivated attacker could target this asset by generating the sufficient conditions to exploit one or more of these vulnerabilities. We use these various assets as the first layer for identifying the potential threats by defining the flaws within each asset.

2) Requirements violation: the exploitation of an existing vulnerability in any asset will lead to a violation in one or more of the security requirements (i.e. Confidentiality, Integrity, or Availability). We could further identify and classify the potential threats based on the violated requirement.

3) Accessibility: finally, the way of accessing the vehicle (i.e., remote, direct, or mixed access) to exploit a specific vulnerability used as the last level for compartmentalization.

Applying this model for the whole vehicle system will identify most of the threats. Achieving each one of these threats will be used as a root of a general attack tree which explains how an attacker could exploit a defined vulnerability. Manipulating the data and disabling the hardware parts in the vehicle are examples of such general attack trees.

These trees will turn into distinct ones gradually reflecting the various studied subsystems. The accomplishment of one

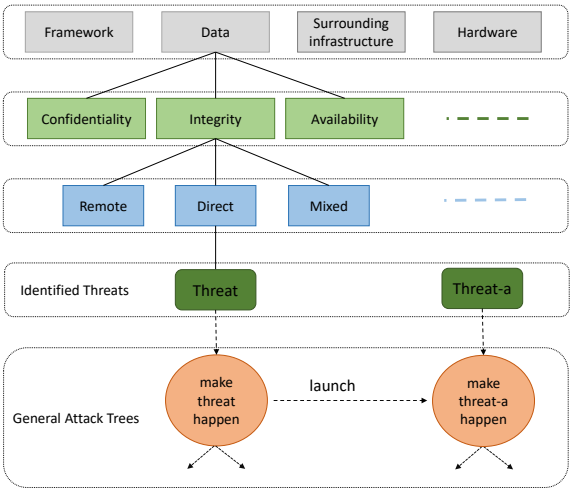

Fig. 1. General threat model which identifies and classifies threats and links them to general attack trees

tree could open the door to fulfill other trees as we explained within the stepping stone attack.

Within the context of a vehicular system, many researchers used attack trees to illustrate the attack vectors which threaten a particular sub-system of the vehicle. However, general attack trees seemed to be indispensable to avoid the redundancy and the interference between the high number of integrated sub-systems within the vehicle. The general trees will be derived from threats which were identified by our proposed threat model.

B. Attack Trees

Threat analysis describes *who* are the potential assaulters, *what* are the motivations behind an attack, and *what* components he could threaten. Describing *How* an attack could occur is the mission of attack trees. An attack tree is used to explain attacks in a tree structure as shown in Fig. 2. The root of the tree represents the essential attacker's goal, while the intermediate nodes of the tree (sub-goals) define different stages of the attack. Each node in an attack tree could require achieving all of its sub-goals. Then the sub-goals are combined by AND branch. Or it could require achieving any one of its sub-goals. In this case, the sub-goals are combined by OR branch. Leafs nodes represent atomic attacks. Attack scenarios are generated from the attack tree by traversing the tree in a depth-first method [14]. Each attack scenario will contain the minimum combination of leafs. The attacks chronology in classical attack tree models was disregarded. But, in many cases, the success of an attack depends on the subsequent success of interrelated attack steps. Arnold et al. [15] proposed the sequential AND- and OR-gates to handle the sequential occurrence of attacks.

C. Review risk analysis

Attack trees were used to evaluate the security risk of the system and calculate the probability of a successful attack. This possibility depends on some aspects, proposed by ISO/IEC 18045, such as the required time for an attack, the

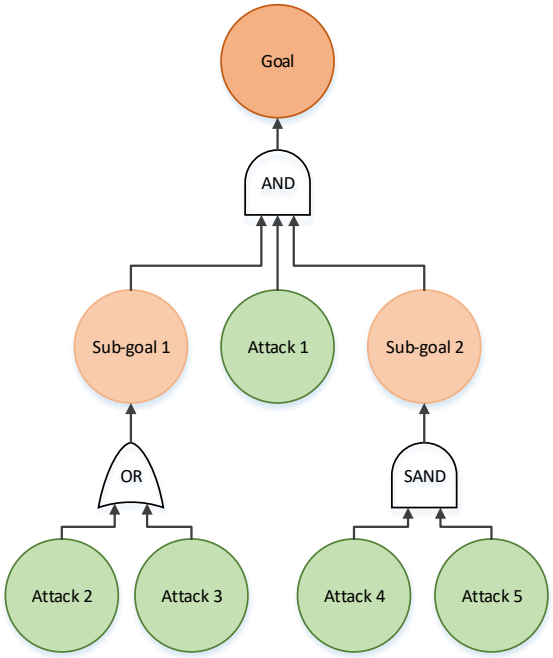

Fig. 2. Attack Tree

desired attack tools, etc. However, regarding the risk analysis within the vehicular domain, the calculation of the probability of potential attacks based on associating numeric values with each level of these factors as proposed by ISO/IEC 18045 is not adequate anymore. Elapsed time, for example, has a different effect regarding the way of carrying out the attack, whether it is a remote attack or one with direct access to the vehicle. Moreover, the overlap between expertise and used tools also has a different effect; even inexpert attacker could launch an attack by using sophisticated tools. finally, the stepping stone attacks should be considered during the calculation of probability of an attack. An attack could have a low likelihood, but achieving one attack goal in a different subsystem may increase this possibility.

IV. Use-case - Automated Obstacle Avoidance

A. Description

In the CCC project, the Institute of Control Engineering (ICE) contributes the full-by-wire research vehicle MOBILE [16] as a demonstrator. MOBILE serves as a platform for research in the fields of E/E-systems and vehicle dynamics. It features four close-to-wheel electric drives (4x100 kW), as well as individually steerable wheels, and electro-mechanic brakes [16]. The vehicle features a FlexRay communication backbone for inter-ECU-communication and additional CAN bus interfaces, which are used for communication with vehicle sensors and actuators. The ECUs responsible for vehicle control are programmed in a custom-designed MATLAB/Simulink tool chain. Combined with detailed vehicle dynamics models, the tool chain serves as a means to establish a rapid-prototyping process for vehicle control algorithms.

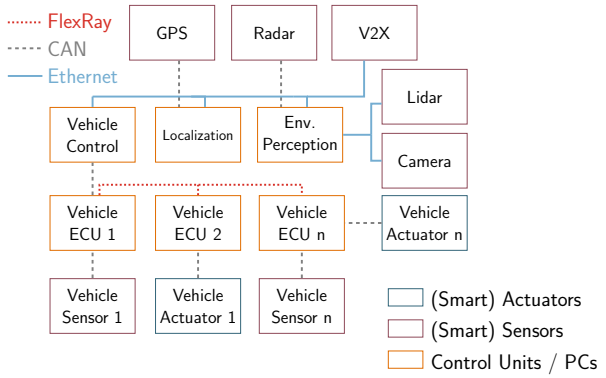

Fig. 3. hardware architecture for obstacle avoidance use-case

Within the scope of the project, a use case in the form of automated obstacle avoidance will be implemented in the experimental vehicle MOBILE. The basis for this use-case is a trajectory following stability control system. In general, stability control systems only steer the vehicle into the direction given by driver input at the steering wheel angle. However, as the driver does not always perform safe steering maneuvers, particularly in critical driving situations, such as fast obstacle avoidance, this extended stability control will follow a safe pre-planned trajectory instead of following a potentially unsafe path, steered by the driver.

The research vehicle is equipped with a variety of environment sensors to perceive the static and the dynamic vehicle environment. Three lidar scanners, a radar sensor and a camera monitor the environment around the car. This data will be used to create a map of the static environment, which provides the basis for a model-based trajectory planning utilizing all actuators (particularly all-wheel steering) for maximal maneuverability.

A hardware architecture showing the perception system, as well as a simplified network for vehicle control is depicted in figure 3. With regard to environment perception, the required actions will be performed in a distributed system of three nodes. GPS and inertial data is fed via CAN to a node which is responsible for vehicle localization and motion estimation. Lidar sensors and a camera are streamed via UDP to a node responsible for environment perception (sensor data processing, data fusion, environment modeling). Data from a radar sensor is aquired via a CAN bus connection.

Trajectory planning will be performed on the ”Vehicle Control” node, utilizing aggregated data from vehicle and environment sensors. The planned trajectory is then converted to reference values for the six vehicle control ECUs (three main control units, three hot stand-by nodes), which are connected with the already mentioned FlexRay backbone. As the research vehicle is not permitted to drive in public traffic, the use-case will be verified and validated on a closed testing ground only. However, the sensor setup and sensor data processing architecture is very similar to the research vehicle *Leonie* [17], also built and maintained by the ICE, so that at least parts of the identified attack vectors could be transferred to a vehicle with a driving permit for public roads.

- Disabling a hardware (availability) (OR)
  - Disabling Camera
    - blinding the camera (SAND)
      - placing LED device
      - emitting a strong light to the camera
  - Disabling sensor or ECUS (OR)
    - transmitting electromagnetic plus (EMP)
    - Crashing the framework of ECU
  - Disabling LIDAR (OR)
    - Jamming LIDAR
    - Physical damage
  - Disabling Radar
    - Jamming attack
- Confusing the proper function of a component
  - Confusing GPS
    - Generating fake GPS signal
  - Confusing LIDAR (OR)
    - spoofing signal
    - replay attack
    - Relaying the signal attack
    - absorbing the signal
  - Confusing Radar (OR)
    - Replaying signal attack
    - Using undetactable obstecale
  - Confusing Camera (OR)
    - Disabling surrounding environment
    - Confusing the auto controls
    - Manipulating surrounding environment

Fig. 4. general attack tree for the Hardware components in our use-case

B. *Threat modeling for the use-case*

We used our model to identify the potential threats within the automated obstacle avoidance use-case. We started our investigation by defining all components which could include vulnerabilities, and identify the security requirement that could be violated in the case of exploiting these vulnerabilities. Lidar, Camera, Radar, and GPS are possible attack surfaces in our use-case. We tried to construct attack trees for each one of them, as shown in figure 4; these trees are derived from the general ones (i.e., disabling a hardware and confusing the proper function of a component). Detailed explanation about attacking the camera and lidar in the vehicle can be found in [18].

The manipulation of the surrounding infrastructures has a direct effect on the functionality of different components in our use-case (such as the Camera). Figure 5 illustrate a general attack tree for the surrounding environment which affect our use-case's components. On the other hand, crashing the framework of an ECU will lead to preventing the ECU from doing its function and disable it, even, temporarily.

V. RELATED WORK

Threats analysis of modern vehicles has remained a hot topic, and will continue. As modern vehicle architecture is getting more complicated, the potential threats are increasing too. Various researchers have tried to point out the vulnerabilities within the vehicular system based on different perspectives; Checkoway et al. [19] looked at potential attack surfaces

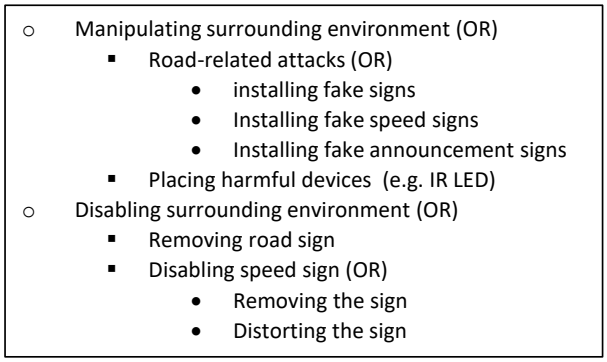

Fig. 5. general attack tree for surrounding infrastructure in our use-case

which could be exploited by attackers externally. On the other hand, Koscher et al. [3] studied the attack surfaces on the underlying system structure. They demonstrated that attackers could leverage the direct access to the CAN bus to control various functions adversarially. Petit and Shladover, in [20], investigate the cyberattacks for the automated and connected vehicle. Attack trees were used as a tool to illustrate the attack steps for individual attack scenarios within the vehicular system such as [9]. Aijaz et al. [21] tried to create a reusable attack tree for the V2V communication threats. In our work, we tried to provide an abstract model which help to create general attack tree for the whole vehicular domain.

Many threat model schemes were used to character cybersecurity threats in different environments,such as STRIDE [22] and SDL [23]. However, McCarthy et at. [24] claimed that these models may not be fully applicable in the automotive cybersecurity analysis. Therefore, they proposed the use of threat model which is a hybrid of various models. We went in the same direction by adopting existing model (i.e. CIA model) in our approach.

VI. Conclusion

In this work, we created a comprehensive threat model based on the existing vehicle-related threat modeling efforts. Our model classifies and identifies the threats based on target assets, the violated security requirements, and the accessibility of the threats. General attack trees can be linked to each of the identified threats. We explored the automated obstacle avoidance use-case while trying to classify the potential threats against it, based on our model. Future work will define mitigation mechanisms based on this model.

Acknowledgement

This work was supported by the DFG Research Unit Controlling Concurrent Change (CCC), funding number FOR 1800. We thank the members of CCC for their support.

References

[1] M. Broy, I. Krüger, A. Pretschner, and C. Salzmann, "Engineering Automotive Software," *Proceedings of the IEEE*, vol. 95, no. 2, 2007.

[2] R. Charette, "This car runs on code," feb 2009. [Online]. Available: http://www.spectrum.ieee.org/feb09/7649

[3] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proceedings of the 2010 IEEE Symposium on Security and Privacy*, ser. SP '10. Washington, DC, USA: IEEE Computer Society, 2010, pp. 447–462.

[4] B. Schneier, "Attack Trees - Modeling security threats," *Dr. Dobb's Journal*, Dezember 1999.

[5] K. Poulsen, "Hacker disables more than 100 cars remotely," Mar 2010. [Online]. Available: https://www.wired.com/2010/03/hacker-bricks-cars/

[6] J. Bogage, "Scary glitch affects luxury cars," JUN 2016. [Online]. Available: https://www.bostonglobe.com/lifestyle/2016/06/09/scary-glitch-affects-luxury-cars/kj4wg2lhphlJDC3gATGuPM/story.html

[7] A. G. Camek, C. Buckl, and A. Knoll, "Future cars: Necessity for an adaptive and distributed multiple independent levels of security architecture," in *Proceedings of the 2Nd ACM International Conference on High Confidence Networked Systems*, ser. HiCoNS '13, 2013.

[8] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *Proceedings of the 19th USENIX Conference on Security*, ser. USENIX Security'10. Berkeley, CA, USA: USENIX Association, 2010.

[9] V. Izosimov, A. Asvestopoulos, O. Blomkvist, and M. Törngren, "Security-aware development of cyber-physical systems illustrated with automotive case study," in *2016 Design, Automation & Test in Europe Conference & Exhibition, DATE 2016, Dresden, Germany*, 2016.

[10] G. Guilbert, E. Jack, R. Karl, and W. Deerek, "Explaining volkswagens emissions scandal," July 2016. [Online]. Available: http://www.nytimes.com/interactive/2015/business/international/vw-diesel-emissions-scandal-explained.html

[11] J. Olofsson, "zombies ahead!a study of how hacked digital road signs destabilize the physical space of roadways," *Visual Communication*, vol. 13, no. 1, pp. 75–93, 2014.

[12] A. Wasicek and W. Andre, "Recognizing manipulated electronic control units," in *SAE 2015 World Congress & Exhibition*, April 2015.

[13] R. Verdult, F. D. Garcia, and B. Ege, "Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer," in *Supplement to the 22nd USENIX Security Symposium (USENIX Security 13)*, 2015.

[14] A. Moore, R. Ellison, and R. Linger, "Attack modeling for information security and survivability," Software Engineering Institute, Carnegie Mellon University, Tech. Rep. CMU/SEI-2001-TN-001, 2001.

[15] F. Arnold, D. Guck, R. Kumar, and M. Stoelinga, "Sequential and parallel attack tree modelling," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2015, pp. 291–299.

[16] P. Bergmiller, "Towards Functional Safety in Drive-by-Wire Vehicles," Ph.D. dissertation, Technische Universität Braunschweig, 2014.

[17] J. Rieken, R. Matthaei, and M. Maurer, "Toward Perception-Driven Urban Environment Modeling for Automated Road Vehicles," in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, Sep 2015, pp. 731–738.

[18] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," in *Black Hat Europe*, 11/2015 2015.

[19] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX Conference on Security*. Berkeley, CA, USA: USENIX Association, 2011.

[20] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16, no. 2, pp. 546–556, 2015.

[21] A. Aijaz, B. Bochow, F. Dötzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmüller, "Attacks on inter vehicle communication systems-an analysis," in *3rd International Workshop on Intelligent Transportation (WIT 2006)*.

[22] Microsoft Developer Networks, "The stride threat model." [Online]. Available: http://msdn.microsoft.com/en-us/library/ee823878(v=cs.20).aspx

[23] ——, "Microsoft security development lifecycle (sdl)." [Online]. Available: ttp://www.microsoft.com/security/sdl/default.aspx

[24] C. McCarthy, K. Harnett, and A. Carter, "Characterization of potential security threats in modern automobiles: A composite modeling approach," Tech. Rep., 2014.