Combining Safety and Security Threat Modelling to Improve Automotive Penetration Testing

Master Thesis Proposal

Michael Wolf

June 12, 2018

1 Motivation

1.1 Research field (Connected autonomous cars)

Three main trends are currently (2018) dominating the car industry.

First, due to the increasing attractiveness of sustainability for consumers and the wish of clean air in the cities, the car manufacturers are shifting their focus from the classic fossil based engines to more eco friendly solutions. This has the effect that many new car models include an electric motor, either as the only driving force or combined with hybrid solutions like a green gas engine or hydrogen fuel cell.

Second, the number of communication technologies for vehicles is increasing. Modern cars have already V2D (Vehicle to Device) communication like the linkage of the mobile phone from the driver with the vehicle via Bluetooth to provide hands-free calling or play-back of audio files. Also, the use of V2C (Vehicle to Cloud) technology is increasing. For example, since April 2018 a system named eCall is now mandatory for new vehicles in Europe which automatically raises an emergency call in case of an accident. Another option is the use of cloud services where vehicle manufacturers distribute updates of their ECU (Electronic Control Unit) over the Internet. Further implementations into newer cars will likely include V2V (Vehicle to Vehicle), V2I (Vehicle to Infrastructure) and V2P (Vehicle to Pedestrian) technologies, where the vehicle informs the environment with data, like it's position and speed, or vice versa, like a person trying to cross the street.

Third, the advanced driver assistance systems (ADAS) are elaborated to automated driving systems (ADS) where the end result will be completely self-driving vehicles. Then, the vehicle does operate without any input of the driver, like acceleration or steering, and even without him monitoring both the road and the car information.

The last two technologies will produce Connected and Autonomous caRs (CARs) which will come with many benefits, like the number of car crashes should drop. This increase of safety comes from both, more data gathered from sensors or communication with external sources which will help the decision making algorithms to better evaluate the current situation, and the reduction of human interaction which are prone to typical human errors. Other benefits are better travel time predictions and better vehicle flow in intersections and therefore reduced energy consumption and an cleaner environment. Furthermore the time in the vehicles can be used for activities because of its connection with the Internet. Even working inside a car becomes a possibility.

However, all these advantages come with new challenges. Due to the increase of ECUs and communication technologies, new threat possibilities arise. Now, not only the safety, but also the security is a topic in the development and testing of vehicles.

1.2 Thesis area (Threat analysis)

To help mitigating the risks of harmful actions and behavior, processes like threat analysis and modelling have been developed. During this process possible vulnerabilities are identified, analyzed and prioritized. This is done by imagining a possible attacker which tries to compromise the system and/ or harm both, the system and the user.

To visualize the data, data flow diagrams are a helpful tool where the entities of the system are displayed and how they interact with each other. Another good graphical format are attack trees, which show conditions which must be fulfilled for an attack to be successful. These conditions can be evaluated how likely they are and then the likelihood of the event can be calculated.

The results of a threat analysis should then help to evaluate from both, the business and security point of view, if and how a potential issue should be fixed. Furthermore it provides a good basis on which tests can be build upon.

A common example is the threat model STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege), developed by Microsoft, which was part of their Security Development Lifecycle which provides a methodology to think about security threats as a part of the whole development, already beginning in the design phase.

However, threat analysis can not only be limited to security, but can also be applied on safety. Car manufacturers are already experienced with risk management, also for the electronic systems. Together with the government they developed the standard for automotive functional safety ISO 26262 [1]. It defines the functional safety of the electric parts in cars and qualitatively rates the risk of dangerous situations. As STRIDE, it is part of the full vehicle lifecycle, from development to retirement.

As than described in Section 2, there already exist some frameworks and models for either, threat analysis for security or safety, but only few are combining both, and none to the authors knowledge are explicitly helping developing future penetration tests. This thesis should address the problem and furthermore provide a tool which should help analyzing the possible threats and designing tests.

2 State of the Art

- A very good introduction into the topic was the Master thesis “Threat Modelling for Future Vehicles, On Identifying and Analysing Threats for Future Autonomous and Connected Vehicles” from Stijn van Winsen [2]. It provides an overview of the vehicular IT components and a general architecture divided on the regions America, Europe and Asia. Furthermore the thesis gives an introduction into threat modelling as well as outlining different approaches, and how an threat model is developed. However, the thesis was about creating an own composite threat model which was evaluated by an security expert of an automotive company. As a nice side benefit, the references of the thesis can be used for more detailed information about certain topics.

- Many papers are referencing the ISO 26262-1:2011 standard [1] which is an international standard for functional safety in electric systems of vehicles. Therefore it would be good to search for other papers which also reference the standard. And because it is “the” standard for functional safety, including it to the evaluation wouldn’t be a bad idea.

- “Automotive functional safety = safety + security.” from Simon Burton et al.[3] is an extension of ISO 26262 which also integrates security aspects. It includes a threat analysis at the beginning phase of the normal Hazard Analysis and Risk Assessment (HARA) and in the end security and safety goals will help to make a better system draft. However, the details on how the threat analysis has to be done, is left to the reader.

- Another holistic approach to co-engineering safety and security is presented by Christoph Schmittner et al. in the article "A Case Study of FMVEA and CHASSIS as Safety and Security Co-Analysis Method for Automotive Cyber-physical Systems" [4]. More specifically, they give a holistic Failure Mode and Effect Analysis solution which extends the safety part with security.
- The interesting article "A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain" from Jürgen Dürrwang et al. [5] points out the problems if the two different worlds of security and safety specialists collide, but they provide a security guided words methodology to help with language problems and therefore let both, security and safety experts identify threats.
- Mozilla developed a web-based application using Node.js and Ruby named SeaSponge [6] to help modelling threats. It provides an UI to draw a data flow diagram. It is hosted on GitHub and open to the public. However, it is very general and more application focused than specific for CARs.
- ThreatDragon [7] is another threat modelling tool. It is distributed for both, a desktop and web application. For the desktop version, electron was used, for the web Angular.js. It has a nice UI, but also a threat/mitigation rule engine. Yet, it needs to be analyzed more, if it can be extended for the use for CARs.

3 Problem Statement

3.1 Thesis focus

As described in Section 2, there already exists some work on threat modelling on both, it-security and functional safety, yet only few combine both for vehicles, especially for connected autonomous cars (CARs). In this thesis, existing tools and processes which help identifying and evaluating threats, an attacker can impose on CARs, should be analyzed and compared with the help of use cases. If none matches the requirements for CARs, an own threat model will be developed. However, the main focus on this model will be on how it can help design and execute penetration tests on CAR, including attack possibilities ranging from an infected cloud server to the option to gain physical access on ECUs inside the car.

To help designing the threat model, a program should be written or an existing extended. This program will have a graphical user interface where the user can add pre-defined components of the car in a diagram and define dependencies and connections between them. Now the program should give the user suggestions of common vulnerabilities and let the user evaluate the probability of such an attack. Furthermore the application should give the user the opportunity to define its own entities and dependencies, as well as populate new vulnerabilities and attack possibilities. Afterwards the diagram can be exported in different formats, from a table with ASILs (Automotive Safety Integrity Levels), to maybe an attack tree, or simply just the diagram as picture.

Both, the model and program will be evaluated by security experts. Employees of Schutzwerk GmbH will be questioned in an expert interview. As a control group, students with IT-Security background and students with no background will also be asked in a survey. Because no personal background experience with designing user studies exists, four weeks are planned for the whole study, from the planning to the evaluation.

3.2 Research questions

Main questions

1. How can the existing methods of safety and security threat analysis be combined?
2. Which existing model fits best for designing penetration tests?
3. Can a tool help with the threat analysis?
4. Can this tool help the following penetration tests?

Knowledge questions

1. What is the architecture of a connected autonomous car?
2. What are security risks?
3. What are safety risks?
4. How can those threats be modeled?

4 Approach

At the beginning more literature will be read. Therefore a full literature search in the databases provided by Uni Ulm will be done as well as promising references looked up, especially those provided in the Master thesis "Threat Modelling for Future Vehicles" of Stijn van Winsen [2]. Also it will be looked a bit into how current threat models for security can be used for helping designing penetration tests, so the adoption to also include safety will be easier.

After the literature gathering, the material will be evaluated and compared to extract a good threat model for CARs. To get a better understanding it will be tried to create an own model and an example analysis will be performed.

During this process, existing tools like SeaSponge [6] or Threat Dragon [7]will be searched and evaluated if they could be extended for this thesis or an own tool needs to be developed. Depending on this decision a CI pipeline will be set up so programming can be done more smoothly afterwards.

5 Planning

5.1 Own Background

For this thesis some knowledge about IT Security is needed, which I have acquired by passing all security courses of the university with the result very good. Special knowledge about cars and the IT systems would be helpful, unfortunately I have not much, except a short introduction to automotive security tests (CAN Bus Testing with CANoe) from Martin Ring, but further knowledge will be gathered through the literature review.

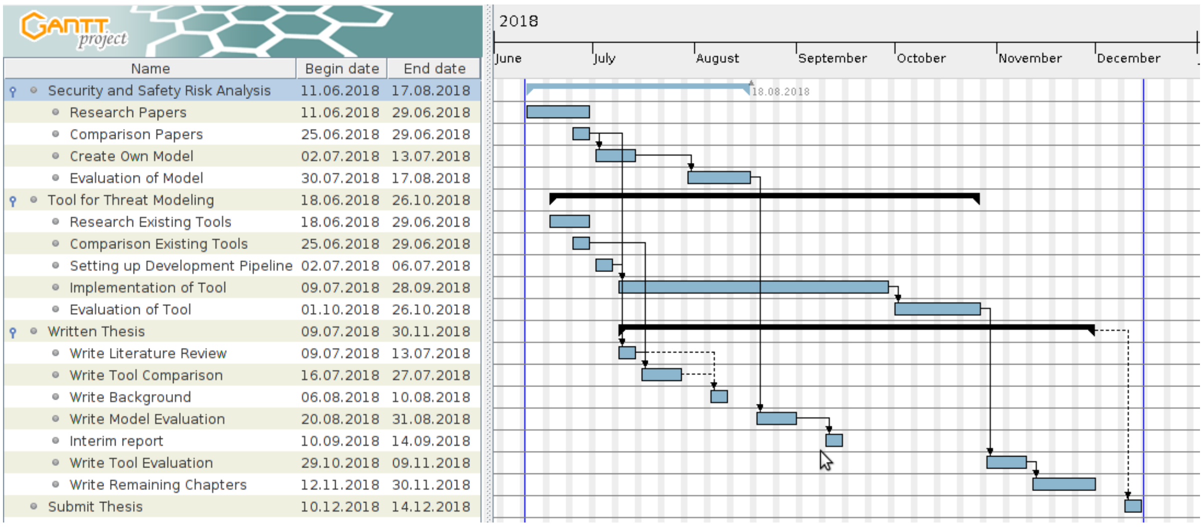
Another skill required, is the ability do develop a program and extend an existing one. There I have a more experience than other students. I was working for three years as software developer and DevOp in a company where I maintained a big website with a team using C# and the .Net Framework, as well as the web technologies HTML5, JS, CSS3. Furthermore I had some student projects where I touched the languages Java, Python and the frameworks Node.js and .Net Core. Hopefully the program will be in one of these known technologies.

5.2 Required Resources

For this thesis only few resources will be needed.

- A Gitlab repository where all documents and the work will be stored. This is already provided by both, Schutzwerk GmbH and the Distributed Systems institute.
- A virtual machine, where the source code (and maybe the latex code) will be compiled and tested. The exact requirements will be known after the comparison of the existing tools (section refsub:wp).
- Further access to research papers which are currently not part of the publishers who have a contract with the university.

5.3 Work packages



Name	Begin date	End date
Security and Safety Risk Analysis	11.06.2018	17.08.2018
Research Papers	11.06.2018	29.06.2018
Comparison Papers	25.06.2018	29.06.2018
Create Own Model	02.07.2018	13.07.2018
Evaluation of Model	30.07.2018	17.08.2018
Tool for Threat Modeling	18.06.2018	26.10.2018
Research Existing Tools	18.06.2018	29.06.2018
Comparison Existing Tools	25.06.2018	29.06.2018
Setting up Development Pipeline	02.07.2018	06.07.2018
Implementation of Tool	09.07.2018	28.09.2018
Evaluation of Tool	01.10.2018	26.10.2018
Written Thesis	09.07.2018	30.11.2018
Write Literature Review	09.07.2018	13.07.2018
Write Tool Comparison	16.07.2018	27.07.2018
Write Background	06.08.2018	10.08.2018
Write Model Evaluation	20.08.2018	31.08.2018
Interim report	10.09.2018	14.09.2018
Write Tool Evaluation	29.10.2018	09.11.2018
Write Remaining Chapters	12.11.2018	30.11.2018
Submit Thesis	10.12.2018	14.12.2018

5.4 Contingency plan

This thesis is also subject to risks.

One can be, that there is no suitable tool, which can be extended by this thesis for threat analysis for security and safety. If this happens, just a backbone with rudimentary functions and no tests or good CI pipeline will be programmed. Or generally spoken, if the development doesn't go as planned, important features will be prioritized over a good looking design.

Another risk factor is the evaluation of the model and tool, when the experts have no time or are getting ill. To mitigate this, multiple experts will also be asked in advance if he will jump in or even better, also do the evaluation.

I personally have no experienced with setting up a user study, so I will follow Bastian Könings advice and try to plan 4 weeks for the study. A risk can therefore be, that not enough time is available for the study. And of course, that a user study may also be the wrong evaluation method and/ or give no clear results. For these scenarios, unfortunately no quick alternative would be available.

References

[1] ISO, *Road vehicles – Functional safety*, Norm, 2011.

[2] S. van Winsen, "Threat modelling for future vehicles, on identifying and analysing threats for future autonomous and connected vehicles," Master's thesis, Kerckhoffs Institute; Faculty of Electrical Engineering, Mathematics and Computer Science University of Twente, 2017.

[3] S. Burton, J. Likkei, P. Vembar, and M. Wolf, "Automotive functional safety = safety + security," in *Proceedings of the First International Conference on Security of Internet of Things*, ser. SecurIT '12, Kollam, India: ACM, 2012, pp. 150–159, ISBN: 978-1-4503-1822-8. DOI: 10.1145/2490428.2490449. [Online]. Available: http://doi.acm.org/10.1145/2490428.2490449.

[4] C. Schmittner, Z. Ma, E. Schoitsch, and T. Gruber, "A case study of fmvea and chassis as safety and security co-analysis method for automotive cyber-physical systems," in *Proceedings of the 1st ACM Workshop on Cyber-Physical System Security*, ser. CPSS '15, Singapore, Republic of Singapore: ACM, 2015, pp. 69–80, ISBN: 978-1-4503-3448-8. DOI: 10.1145/2732198.2732204. [Online]. Available: http://doi.acm.org/10.1145/2732198.2732204.

[5] J. Dürrwang, K. Beckers, and R. Kriesten, "A lightweight threat analysis approach intertwining safety and security for the automotive domain," in *Computer Safety, Reliability, and Security - 36th International Conference, SAFECOMP 2017, Trento, Italy, September 13-15, 2017, Proceedings*, 2017, pp. 305–319. DOI: 10.1007/978-3-319-66266-4_20. [Online]. Available: https://doi.org/10.1007/978-3-319-66266-4_20.

[6] Mozilla. (2015). Seasponge, [Online]. Available: https://github.com/mozilla/seasponge (visited on 06/11/2018).

[7] M. Goodwin. (2017). Owasp threat dragon, [Online]. Available: https://github.com/mike-goodwin/owasp-threat-dragon (visited on 06/11/2018).