Practical Security and Privacy Threat Analysis in the Automotive Domain: Long Term Support Scenario for Over-the-Air Updates

Alexandr Vasenev[1], Florian Stahl[2], Hayk Hamazaryan[3], Zhendong Ma[4], Lijun Shan[5],
Joerg Kemmerich[3] and Claire Loiseaux[5]
[1]*ESI (TNO), Netherlands*
[2]*AVL Software & Functions, Germany*
[3]*ZF Friedrichshafen AG, Germany*
[4]*AVL, Austria*
[5]*Internet of Trust, France*

Keywords: Data Flow Diagram, STRIDE Taxonomy, LINDDUN Methodology, UNECE Threat Catalogue, Risk Management.

Abstract: Keeping a vehicle secure implies provide of a long-term support, where over-the-air updates (OTA) play an essential role. Clear understanding of OTA threats is essential to counter them efficiently. Existing research on OTA threats often exclude human actors, such as drivers and maintenance personnel, as well as leave aside privacy threats. This paper addresses the gap by investigates security and privacy OTA threats relevant for vehicle manufacturers for the whole product lifecycle. We report on a practical scenario “long term support”, its data flow elements, and outcomes of threat analyses. We apply state of the art approaches, such as STRIDE (extended with an automotive template) and LINDDUN, to an automotive case and consider an automotive-specific UNECE OTA threat catalogue. Outcomes indicate complementarity of these methods and provide inputs to studies how well they address practical automotive cases.

1 INTRODUCTION

The automotive industry has taken a tremendous technology leap in recent years with innovations targeting low emission, autonomy, and smart mobility. This has led to a significant increase in electronics and software in and around the vehicle that shall function properly during the car lifecycle.

Driven by requirements from external parties and search for financial benefits, automotive companies consider long term support (LTS) strategies to keep a vehicle secure. ISO/IEC 12207 (2017) highlights the LTS relevance for stable SW releases. Over-the-air software updates (OTA) are essential elements of LTS. One OEM (Original equipment manufacturer) positions them as follows: “With our over-the-air software updates, remote diagnostics and the support of our Mobile Service technicians, we reduce the need to visit a Service Center” (Tesla, 2019).

OTA brings benefits to vehicle users, OEMs, and maintenance personnel. Features of remote updates (such as location-independence, cost efficiency, and short time from release to update) provide users with updated functions and can even improve core safety features, e.g., breaking distances (O'Kane, 2018). Maintenance personnel benefit by eliminating time needed to connect wires.

Research on OTA, e.g. (Schmidt et al., 2018) and (Idrees et al., 2011), often focus on technical difficulties, such as bootloaders, ECUs (Electronic Control Unit), and in-vehicle networks. A challenge remains how to design OTA schemes that satisfy all automotive demands (Van Huynh Le et al., 2018).

In our view, studying OTA systematically can help to inform research how to address this challenge. Current literature lacks descriptions of realistic LTS scenarios with systematic analysis of OTA security and privacy threats. This paper addresses this gap. We do so by applying state of the art approaches to the automotive domain.

2 BACKGROUND

Security is one of the biggest challenges for OTA updates due to the severity and liability of potential

Vasenev, A., Stahl, F., Hamazaryan, H., Ma, Z., Shan, L., Kemmerich, J. and Loiseaux, C.
Practical Security and Privacy Threat Analysis in the Automotive Domain: Long Term Support Scenario for Over-the-Air Updates.
DOI: 10.5220/0007764205500555
In *Proceedings of the 5th International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS 2019)*, pages 550-555
ISBN: 978-989-758-374-2

negative consequences. An OTA update system must be resilient to spoofing, tampering, repudiation, information-leakage, denial-of-service, and escalation-of-privileges attacks (FASTR, 2018). As demonstrated, hackers can compromise current OTA update technology and take complete control of a road vehicle (Miller&Valasek, 2015).

Significant research efforts focus on technical OTA aspects. Lewis (2010) investigated OTAs and associated security protocols. Idrees et al. (2011) described a hardware security module to protect critical architecture elements during firmware updates, such as secure key storage and secure operation of cryptographic algorithms. Schmidt et al. (2018) considered a bootloader for secure remote firmware updates. Steger et al. (2016) proposed a generic framework to enable secure and efficient wireless automotive SW updates for vehicle's lifetime. Several stages and roles were covered, namely Engineers (Product development), Operator (Assembly line), and Mechanic (Workshop).

Securing OTA also demands considering engineering and operation perspectives. Examples include secure communication architecture (Papadimitratos et al., 2008), engineering method (Schmittner et al., 2015), risk management (Schmittner et al., 2016), and automotive threat modelling (Ma & Schmittner, 2016).

This paper extends the existing research by focusing on OTA problem space exploration using state of the art cybersecurity methods described next.

2.1 Security Analysis Methods

Security is essential for safety critical systems, such as vehicles. SAE J3061 (2016) provides guidelines on security engineering based on the vehicle functional safety engineering framework from ISO/IEC 26262 (2011). SAE recommends several security analysis techniques oriented to automotive, e.g. EVITA, TVRA, OCTAVE, and HEAVENS.

The latter employs a well-known security STRIDE threats and advocates an integrated security-safety analysis. STRIDE defines both a threat model and a stepwise process of threat modeling. As a threat model, it provides a mnemonic for security threats in six categories: Spoofing of user identity, Tampering, Repudiation, Information disclosure (privacy breach or data leak), Denial of service, Elevation of privilege. STRIDE has been widely applied to analyze the security of systems, since it provides a clear classification of threats.

As a threat modelling process supported by a software tool, STRIDE starts from the functional description of a system in the form of DFD (data flow diagram), then derives a set of threats by applying STRIDE threat categories.

The identified threats can be ranked. E.g., SAHARA method (Macher, 2016) considers the Level of Knowledge and Resources required for an attack with the Threat Criticality (e.g., annoying, damage of goods, life-threatening). The resulting Security Levels (from 1 – 4, where 4 is the most critical) help to decide how risks should be treated with which security goals and requirements.

In addition to performing a step-wise process for identifying threats e.g. STRIDE, one can consult existing threat catalogues developed by experts for certain types of systems, e.g., (Unece, 2018).

2.2 Privacy Analysis Methods

Privacy focus on protecting data related to people (i.e., personal data). Examples include name, address, email, location, driving behavior, license number, relations to other people (friends), or health information. Currently, no internationally standardized privacy engineering method exists for automotive. ISO 27550 (under development) is the first international method that focus on such concerns for information systems. It specifies principles privacy-by-design and privacy-by-default, as well as the processes for identifying, evaluating and treating privacy risks in the course of systems design. ISO 27550 recommends several privacy risk analysis techniques, e.g. the CNIL privacy model, PRIPARE, and LINNDUN method (Kim&Joosen, 2015).

LINDDUN (https://linddun.org/) is a method for privacy threat analysis that follows several steps: 1. Define DFD; 2. Map privacy threats to DFD elements; 3. Identify threat scenarios; 4. Prioritize threats; 5. Elicit mitigation strategies; 6. Select corresponding privacy-enhancing technologies. Similarly to STRIDE, LINDDUN builds on DFD elements (an entity, data store, data flow, and processes) and associated with a number of privacy threat categories abbreviated in its name (Likability, Identifiability, Non-repudiation, Detectability, information Disclosure, content Unawareness, and policy and consent Non-compliance).

Several of the mentioned security and privacy analysis methods were used in the reported research as described next.

3 ANALYSING A USE CASE

For analyzing the LTS scenario with OTA, we followed the approach adopted in the Secredas (http://secredas.eu/) project. We applied STRIDE for the security assessment and LINDDUN for the privacy assessment. Both are established approaches that employ DFD (Table 1) for identifying threats. STRIDE is supported by a SW tool to automatically generate lists of threats.

Table 1: The adopted analysis method.

	Security	Privacy
Analysis method	STRIDE	LINDDUN
Input	DFD	
	UNECE matrix	
Output	Prioritized security threats	Prioritized privacy threats

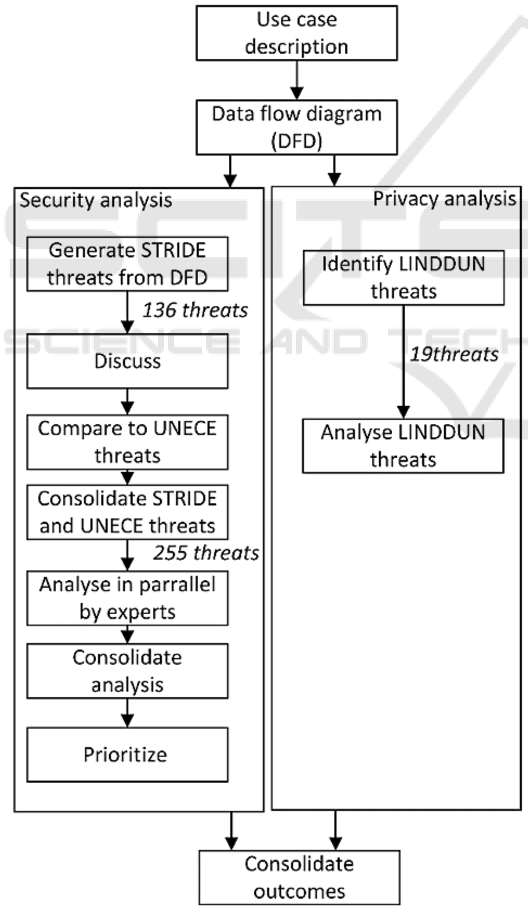

Figure 1: The Flow of the analysis.

We conducted our analysis as illustrated in Figure 1. To complement STRIDE, we took into the UNECE threat catalogue on OTA threats. To rank security threats we applied the SAHARA method. For privacy analysis, we followed LINDDUN's steps 1-3 (problem space) and 4 (prioritize- first solution step).

3.1 Use Case Description

We structured the process of handing security and privacy issues for the LTS scenario as follows. Once a critical cybersecurity bug is detected, label management identifies affected HW and SW components. Case triage assesses the vulnerability. A decision follows whether to start the bug fix procedure or just document the bug. Once a patch (or new HW) is available, a bulletin is broadcasted to necessary parties. *Vehicle gateway* (items in italic are of major interest for the following analysis), located within the vehicle boundary, checks the *OEM cloud* regularly for new updates. If an HW update or a new SW requires a manual update, the *driver* will be notified that a HW change or a manual SW update is available and required. He or she will need to make an appointment at a *service station.*

Vehicle gateway follows OTA steps:

- If an update is available, check compatibility and legitimation;
- If check is positive, *Gateway* notifies *Driver* a new update is available;
- If *Driver* confirms update, *Gateway* downloads the update from *OEM server*, verifies its cryptographic signature;
- *Gateway* initiates an ECU software update over the *CAN bus*;
- If ECU update is successful, *Gateway* notifies *Driver*, *Gateway* also notifies the backend server that a new version of update is installed on the vehicle.

3.2 Data Flow Diagram

Based on the use case description, we built the data flow diagram with assets and data flows. For creating the diagram we used MS Threat Modelling Tool that supports automated STRIDE threat analysis with the Automotive Threat Modelling Template (Nccgroup, 2017). Figure 2 indicates flows within and across boundaries of the OEM cloud, Service station, car, and OEM backend. To provide a stable base for analysis using the STRIDE methodology, we generalized design of assets located in common areas like vehicle and OEM cloud. OEM backend was not detailed to keep focus on the vehicle.

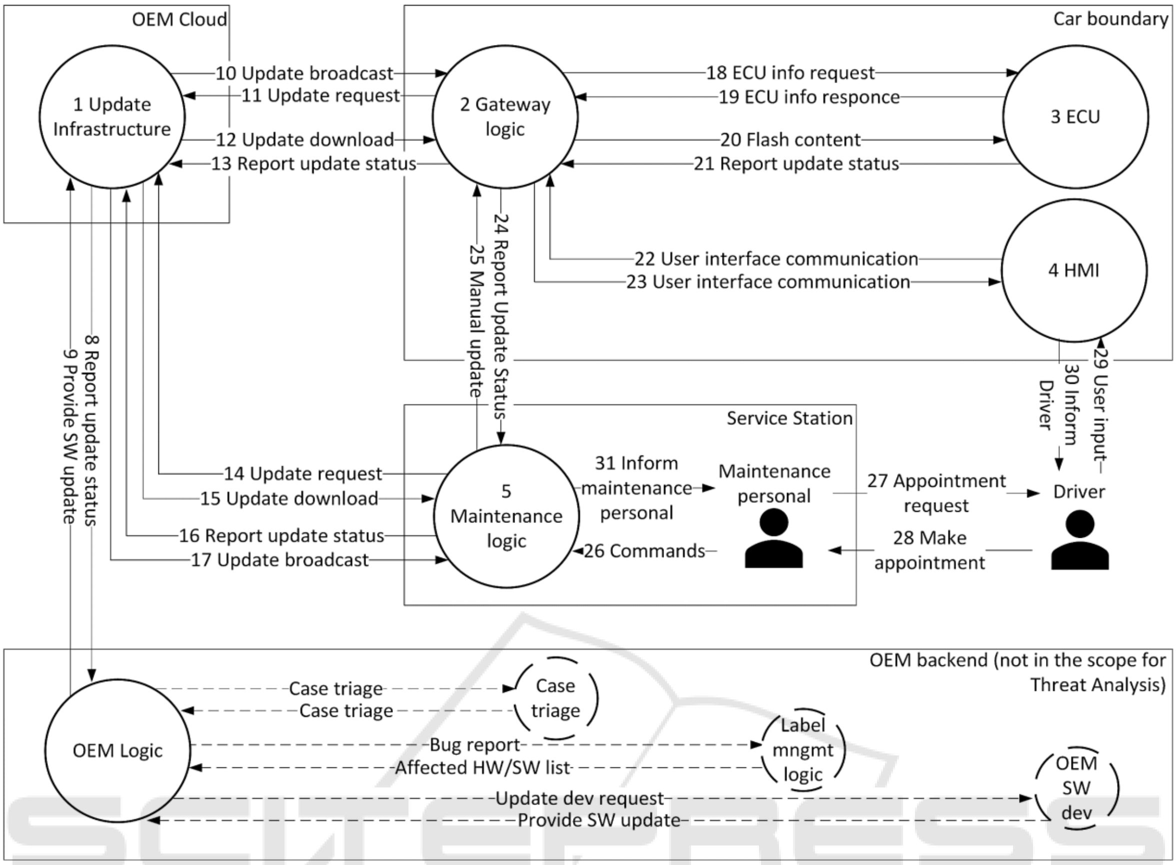

Figure 2: Data flow diagram of the long term support scenario.

3.3 Security and Analysis Steps

As noted in Figure 1, we generated a list of 136 security threats using the MS Threat Modelling Tool. We reviewed and discussed threats in an expert group meeting. Threats were filtered and grouped manually to remove duplicates, checked for missing or inappropriate threats. Threat descriptions were adjusted to better reflect our use case.

Then, we compared the list of STRIDE threats with threats listed by UNECE. We identified each STRIDE threat in the UNECE list. Afterwards, we selected only UNECE threats relevant to our use case. By synchronizing and combining lists, we obtained 255 threats. To handle such a high number of threats, we split the work among team members and prioritized threats using a method based on SAHARA.

3.4 Outcomes

Table 2 shows an extract of the final list of threats, generated using STRIDE (‘SecLevel’ stays for SAHARA Security Level). Table 3 illustrates threats found with the UNECE threats catalogue that were not identified when STRIDE was applied to the DFD.

Table 2: Some of CAN BUS (18-23) tampering threats.

Threat Scenario	SecLev
Unauthorized deletion/manipulation of system events log	1
Introduce malicious software or malicious software activity	2
Fabricating software of the vehicle control system or information system	1
Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a malicious payload	3
Unauthorized access or falsify the configuration parameters of vehicle’s key functions, such as brake data, airbag deployed threshold, etc.	2

Two privacy experts analyzed threats to personal data in the outlined LTS case. The application of the LINDDUN method resulted in 19 threats. Table 4 lists a subset of them.

Table 3: UNECE Threats to vehicles regarding unintended human actions.

Threat Scenario	SecLev
Misconfiguration of equipment or systems by driver	2
Misconfiguration of equipment by maintenance	4
Defined security procedures are not followed (by driver or maintenance personnel)	4
Innocent victim (e.g. owner, operator or maintenance engineer) being tricked into taking an action to unintentionally load malware or enable an attack	2

Table 4: Extract of LINDDUN privacy threats.

LINDDUN threat	threat scenario	Priority
Maintenance personnel		
Information Disclosure	The appointment request can be eavesdropped on	Low
Non-Repudiation	Show that the driver was in contact with maintenance personnel	Low
Content Unawareness	Privacy information is not shown to the maintenance personnel in an easily understandable way.	Low
Driver		
Content Unawareness	Privacy information is not shown to the car user in an easily understandble way.	High
Linkability	A driver contacting maintenance personnel infers that there is a is a problem with the car. This can be very interesting information for an attacker.	Low
Update Infrastructure		
Linkability	Data not required for maintenance purposes (e.g. precise location) is transferred to the OEM and can be mapped to the car user	High
Information Disclosure	Personal data of car users can be revealed if an attacker gets access to the update infrastructure	High

Tables 2-4 illustrate the complementarity of different approaches. Table 2 lists threats illustrative for STRIDE that adequately represents threats to a HW/SW system. Table 3 includes accidental errors. Such threats are not part of the STRIDE taxonomy, but are relevant for LTS OTA updates. They account for human actions in the system and complement the system-level analysis. Privacy threats (Table 4) are linked to human actors, but do not originate from the actors in the scenario. This dimension of relevant threats is hard to find using other methods.

4 DISCUSSIONS

During the security analysis, we noted that the used Automotive Threat Modelling Template detected many important threats. It assumed CAN as being insecure, which is directly relevant for the analysis. Yet, manual adjustments was needed because:

- The template focuses on V2X communication and is not the best fit for OTA updates;
- Human actions and social engineering threats are not covered;
- Spoofing and Repudiation threats are less visible.

The UNECE list covered all threats identified with the STRIDE approach, yet required to make some assumption on how such threats are connected. UNECE provided additional coverage of misconfiguration and spoofing threats.

For the privacy threat analysis neither a tool to automatically generate threat lists nor a comprehensive (UNECE-like) list of threats was available. This suggests that the privacy topic in the automotive domain has not reached the same level of maturity as cybersecurity.

We observed that outcomes of our security and privacy analysis overlap. While some privacy threats were new, others appeared similar to security issues identified before. This is expected, as security and privacy analysis look at the confidentiality of data, but the points differ: privacy concerns the personal data, while security covers all data.

5 FUTURE WORK

The conducted analysis has its limits. To scope the case, we focused on the OEM Cloud, vehicle, service station, and the driver. We left outside bug detection, case triage, update development, management for different Tier1 suppliers, branching, and update broadcast. We did not define technical details for communication and hardware. Besides, LTS in the automotive domain includes hardware and can concern different ways of rollout. Other research may scope the analysis differently.

Future research might consider how to include social aspects into analysis of cyber-physical systems. Although we did include people (driver and maintenance) and considered unintentional threats using LINDDUN, a more structured approach to conduct analysis might be developed.

6 CONCLUSIONS

This paper outlined a realistic case to keep a vehicle secure for its lifecycle. Privacy and security threats for OTA updates were analyzed with the aim to inform discussions on long-term support threats and relevant tools.

We observed that outcomes of state of the art methods are useful and complement each other. Yet, our experience shows that the used methods still lack application guidelines and templates appropriate for threat modeling of automotive systems. Future research can address these gaps.

ACKNOWLEDGEMENTS

This work is supported by the H2020-ECSEL programme of the European Commission; grant no. 783119, SECREDAS project. Teun Hendriks made valuable remarks on an earlier paper version.

REFERENCES

FASTR, 2018, *Automotive Industry Guidelines for Secure Over-the-Air Updates*, April 2018

Idrees, Sabir & Schweppe, Hendrik & Roudier, Yves & Wolf, Marko & Scheuermann, Dirk & Henniger, Olaf. 2011. *Secure Automotive On-Board Protocols: A Case of Over-the-Air Firmware Updates*. pp. 224-238.

ISO12207, 2017. International Organization for standardization, *ISO/IEC/IEEE 12207:2017, Systems and software engineering -- Software life cycle processes*, *https://www.iso.org/standard/63712.html*. Last accessed: Jan 2019.

ISO26262, 2011, *26262: Road vehicles-Functional safety*. International Standard ISO/FDIS 26262

Kim, Wuyts, Joosen, Wouter, 2015 *LINDDUN privacy threat modeling: a tutorial*.

Lewis, Derek Lane, 2010, *Over-the-air vehicle systems updating and associate security protocols*, patent US9464905B2, priority date: 2010-06-25

Ma Z., Schmittner, C., 2016, *Threat Modeling for Automotive Security Analysis*, SecTech 2016, 2016

Macher, Georg, Armengaud, Eric, Brenner, Eugen, Kreiner, Christian, 2016, *Threat and Risk Assessment Methodologies in the Automotive Domain*, Procedia Computer Science, Volume 83, 2016, Pp. 1288-1294,

Miller, C. Valasek, C., 2015, *Remote exploitation of an unaltered passenger vehicle*, August 2015, available: *http://illmatics.com/Remote%20Car%20Hacking.pdf*, last accessed: Jan 2019

Nccgroup, 2017, *Automotive threat modeling template*, *https://github.com/nccgroup/The_Automotive_Threat_ Modeling_*Template, last accessed: Jan 2019.

O'Kane S., 2018, *Tesla can change so much with over-the-air updates that it's messing with some owners' heads*, *https://www.theverge.com/2018/6/2/17413732/tesla-over-the-air-software-updates-brakes*, acc.: Jan 2019.

Papadimitratos, P., Buttyan, L., Holczer, T., Schoch, E., Freudiger, J., Raya, M., Ma, Z., Kargl, F., Kung, A., Hubaux, J.-P., 2008, *Secure Vehicular Communication Systems: Design and Architecture*, IEEE Communications Magazine, vol. 46, no. 11, pp. 100--109, November 2008

SAE, 2016, Vehicle Electrical System Security Committee. *SAE J3061-Security Guidebook for Cyber-Physical Automotive Systems*.

Schmidt, Silvie & Tausig, Mathias & Koschuch, Manuel & Hudler, Matthias & Simhandl, Georg & Puddu, Patrick & Stojkovic, Zoran, 2018, *How Little is Enough? Implementation and Evaluation of a Lightweight Secure Firmware Update Process for the Internet of Things*. 10.5220/0006670300630072.

Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., Puschner, P., 2016, *Using SAE J3061 for automotive security requirement engineering*, In International Conference on Computer Safety, Reliability, and Security, pp. 157-170. Springer International Publishing, 2016

Schmittner, C., Ma, Z., Gruber, T., 2015, *Combining Safety and Security Engineering for Trustworthy Cyber-Physical Systems*, ERCIM News 2015(102)

Steger, M., Karner, M., Hillebrand, J., Rom, W., Boano C., and Römer, K., 2016, *Generic framework enabling secure and efficient automotive wireless SW updates*, IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), Berlin, pp. 1-8.

Tesla, 2019, *Vehicle Warranty*, *https://www.tesla.com/ support/vehicle-warranty*, last accessed: Jan 2019.

UNECE, 2018, *Draft Recommendation on Software Updates of the Task Force on Cyber Security and Over-the-air issues of UNECE WP.29 IWG ITS/AD*. *https://www.unece.org/fileadmin/DAM/trans/doc/2018 /wp29grva/GRVA-01-17.pdf*, accessed: Jan 2019.

Van Huynh Le, Jerry den Hartog, Nicola Zannone, 2018, *Security and privacy for innovative automotive applications: A survey*, Computer Communications, Volume 132, 2018, Pages 17-41, ISSN 0140-3664.