Threat Modeling and Attack Simulations of Connected Vehicles: Proof of Concept

Wenjun Xiong(✉), Fredrik Krantz, and Robert Lagerström

School of Electrical Engineering and Computer Science,
KTH Royal Institute of Technology, Stockholm, Sweden
{wenjx,fkra,robertl}@kth.se

Abstract. A modern vehicle contains over a hundred Electronic Control Units (ECUs) that communicate over in-vehicle networks, and can also be connected to external networks making them vulnerable to cyber attacks. To improve the security of connected vehicles, threat modeling can be applied to proactively find potential security issues and help manufacturers to design more secure vehicles. It can also be combined with probabilistic attack simulations to provide quantitative security measurements, which has not been commonly used while shown efficient in other domains. This paper reviews research in the field, showing that not much work has been done in the combined area of connected vehicles and threat modeling with attack simulations. We have implemented and conducted attack simulations on two vehicle threat models using a tool called securiCAD. Our work serves as a proof of concept of the approach and indicates that the approach is useful. Especially if more research of vehicle-specific vulnerabilities, weaknesses, and countermeasures is done in order to provide more accurate analyses, and to include this in a more tailored vehicle metamodel.

Keywords: Threat modeling · Attack simulations · Vehicles · Cyber security

1 Introduction

Modern vehicles are often connected to the Internet, and they contain more than 100 Electronic Control Units (ECUs) that control brakes, airbags, parts of the engine, and so on. This combination of ECUs, sensors, and network buses creates a computerized system. Vehicles seem to be vulnerable to exploits in several ways, and a malicious actor getting access to vital ECUs can have dire safety consequences. Vehicle vulnerabilities have been reported numerous times, e.g. in the National Vulnerability Database (NVD)[1]. One famous example of exploiting vehicle vulnerabilities is when two ethical hackers acquired remote control of a 2014 Jeep Cherokee[2].

[1] https://nvd.nist.gov/.
[2] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

P. Mori et al. (Eds.): ICISSP 2019, CCIS 1221, pp. 272–287, 2020.
https://doi.org/10.1007/978-3-030-49443-8_13

To improve the security of Internet-facing systems e.g. vehicles, one approach is to use methods for modeling and analysis. One can with this understand what parts of the system are the most weak ones, and how they can be secured. Threat modeling is one such way of working with proactive cyber security and security by design [34], moreover, the most recent trend is to combine it with attack simulations to provide quantitative security measurements [13,33], e.g. Time-To-Compromise (TTC) [7,10]. This fairly new approach has been applied successfully in domains like energy [30]. This paper serves as a proof of concept of the approach on connected vehicles.

A threat modeling and risk management tool called securiCAD[3] is used in this work, where users can model e.g. home Local Area Networks (LANs), large corporate networks, and SCADA systems. In securiCAD, different defense strategies are assigned to different assets, and the built-in simulation engine is used to show the probabilities of different attacks succeeding. Some attack types that can be simulated include Denial of Service (DoS), device compromise, and replay attacks [6]. Furthermore, our literature review and practical tests using securiCAD show that threat modeling and attack simulations for vehicles is promising, while some aspects need to be further considered in future research for it be more efficient and successful.

This paper is an extension of the paper presented at the 5th International Conference on Information Systems Security and Privacy in Prague, Czech Republic [33]. The extension includes: 1) related work on vehicle privacy is added in Sect. 2; 2) more detailed vehicle threat modeling steps and one more vehicle model is added in Sect. 3; 3) further described simulation results for the vehicle models in Sect. 4; 4) further discussed proof of concept in vehicle threat modeling and attack simulations in Sect. 5, and more detailed conclusions in Sect. 6.

2 Related Work

2.1 Threat Modeling and Attack Simulations

Threat modeling is proposed as a solution for secure application development and system security evaluations, and it aims to be more proactive and make it more difficult for attackers to accomplish their malicious intents. The work by Shostack [26] and the Microsoft Threat Modeling tool[4] are commonly used in this area. In [31], the authors studied the usefulness of the Microsoft Threat Modeling tool and showed that the tool improved their work on threat modeling. However, it is mainly used for designing secure software applications, and often not for considering the system from a holistic point of view. In [27], SPARTA was proposed to combine Data Flow Diagram (DFD)-based threat modeling with security and privacy solutions. Risk analysis simulations based on concrete element value estimates, countermeasure strengths, and attacker types provide a prioritized list of threats that should be elicited.

[3] https://www.foreseeti.com/.
[4] https://www.microsoft.com/en-us/download/details.aspx?id=49168.

Another way of working with threat modeling is to use attack trees or attack graphs [14,23,25]. Attack graphs are widely accepted and used, while there are plenty of known problems. For instance, in [19] the authors stated that previous work on attack graphs has not provided an account of the scalability of the graph generating process, and there is often a lack of logical formalism in the representation of attack graphs, which results in the attack graph being difficult to use and understand by human beings. As a response to these known problems in threat modeling and attack simulations, some approaches have been proposed. For example, pwnPr3d [10] and MAL (the Meta Attack Language) [7] were proposed focusing on providing probabilistic security measures.

2.2 Vehicle Security and Privacy

Previously, vehicle Original Equipment Manufacturers (OEMs) did not consider cyber attacks that much, since an attack was only possible if an attacker had physical access to the vehicle. However, as modern vehicles have multiple wireless connections to both outside networks and devices (e.g. Bluetooth, Internet), they are vulnerable to cyber attacks[5]. Some vehicle vulnerabilities are recorded in NVD, and each of them is associated with a CVE[6] number and CVSS score[7] for analyzing its severity.

To help improving the security of modern vehicles, [32] conducted an empirical study to identify common security vulnerabilities discovered in vehicles. The vulnerability information was gathered for 60 vehicle OEMs and common vehicle components from NVD. The analysis results showed that about 50% of the vulnerabilities fall into the medium severity category, and the three most common software weaknesses reported are protection mechanism failure, buffer errors, and information disclosure.

By using threat modeling for vehicles, the process proposed by [20] starts with defining automotive security use cases, then identifying assets and threats by using the STRIDE method, and finally rating risks and evaluating the threat level and impact level against the found threats. Besides, for assessing the risks of exploiting vehicular on-board networks, [24] automatically generated and analyzed attack graphs, which could aid vehicle development by automatically rechecking the architecture for attack combinations. In [12] the authors adapted two threat modeling methods - TARA and STRIDE from the computer industry to fit the needs of the automotive industry. Also, in [16] an approach to threat modeling to better fit the automotive systems was proposed, a proof of concept implementation of their approach was implemented but without further validation.

Possible security mechanisms to secure vehicles internal communications were addressed in the Holisec project[8], including message authentication codes (MAC)

[5] https://www.cpomagazine.com/cyber-security/connected-cars-a-new-and-dangerous-vector-for-cyber-attacks/.
[6] https://cve.mitre.org/.
[7] https://www.first.org/cvss/.
[8] http://autosec.se/wp-content/uploads/2018/04/1.2-holisec-state-of-the-art.pdf.

for traffic integrity, firewalls both for external traffic and for internal traffic implemented in gateway ECUs, use of Intrusion Detection Systems (IDSs) to detect unusual activities on the networks, and certificates for identification of various devices. Security mechanisms were also addressed in [3] to mitigate the threats on assets, which include access control, packet filter firewall, message authentication, etc. Considering the privacy issues of vehicular data, the work by [35] presented a privacy specification for vehicles, which used MAL [7] to assess the security of connected vehicles with a special focus on the privacy aspect.

3 Vehicle Threat Modeling

According to a survey conducted by Miller and Valasek [17], the two most hackable vehicle models are the 2014 Jeep Cherokee and 2015 Cadillac Escalade. Therefore, these two models are used for our proof of concept work.

The threat modeling is done using securiCAD, a tool that can automatically generate probabilistic attack graphs from a given system specification, and serves as an inference engine that produces predictive security analysis results. The threat models can be built by using drag-and-drop functionality with pre-defined assets and associations. Each asset has certain security properties and attack types associated with it. For example, a `Network` asset has e.g. DoS, ARP cache poisoning, and compromise attacks listed.

3.1 Creating Threat Models

For modeling and analyzing vehicles, the first thing is to understand the internal network of a vehicle, and the main assets in it. The main assets in a connected vehicle include `ECU`, `SoftwareProduct`, `Dataflow`, `Protocol`, and `Network`. The most common `Protocol`s in vehicle communication include CAN, LIN (Local Interconnect Network), MOST (Media Oriented Systems Transport), and FlexRay.

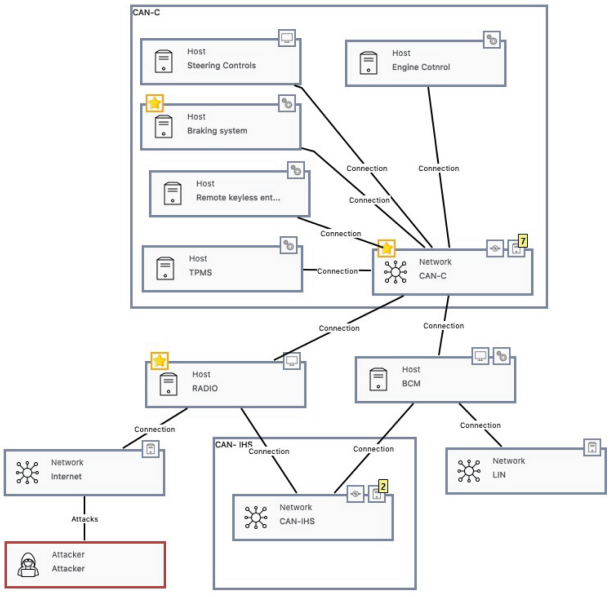
A `Host` is described as a kernel of an operating system in securiCAD, and is used to represent PCs or servers, thus here it is used to represent `ECU`s. In order to model the associations between the assets, a `Service` and a `Client` can be connected to each `ECU`, while an `ECU` does not require both of them, e.g. an `ECU` will be connected to a `Client` only if it is required to send data to other `ECU`s.

The software used on these `ECU`s is either made entirely by the OEMs, or applies existing architecture standards to define the functions of each `ECU`, e.g., AUTOSAR[9], which is a standardized software framework for vehicles and offers a multi-level security architecture among others. Many OEMs and third-party developers are members of AUTOSAR today and the number of members is still growing [5,11]. Therefore, a `SoftwareProduct` that represents AUTOSAR is connected to each `ECU`, as well as its `Service`s and `Client`s. Moreover, `Dataflow`

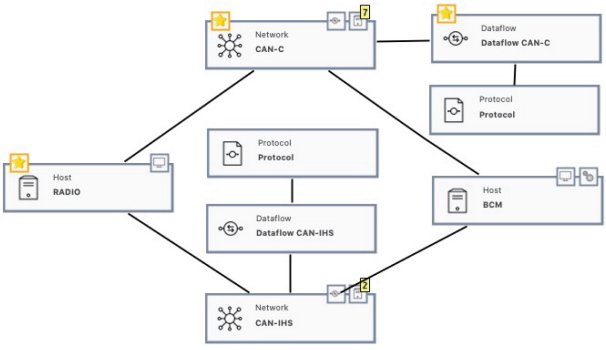
[9] https://www.autosar.org/.

is connected to each `Network`, and is also connected to `Service`s and `Client`s of `ECU`s to represent the communication between them. The communication here denotes the access that `Service` and `Client` have to the commands and function calls in the kernel. The following two examples show how we created the threat models and the reasoning behind it.

2014 Jeep Cherokee Model. The 2014 Jeep Cherokee threat model is created according to its network topology [17]. As is shown in Fig. 1(a), the vehicle network topology contains two CAN `Network`s (CAN-C, CAN-IHS) and one LIN



(a) Network topology viewpoint [33]



(b) Dataflow viewpoint

Fig. 1. 2014 Jeep Cherokee threat modeling.

Network. CAN-C is a Low Speed CAN Network that connects ECUs e.g. steering controls, brakes, tire pressure monitoring system (TPMS) that are considered safety-critical. CAN-IHS is an Interior High Speed CAN Network that connects the comfort systems e.g. radio, climate controls. The LIN Network connects ECUs e.g. rear view mirror, and lamps. Also, a RADIO box is connected to these two CAN Networks.

A Body Control Module (BCM) connects both of the two CAN Networks and the LIN Network. It ensures the information exchange in spite of different of data transmission rates in each network. Also, we connect it to Dataflow (see in Fig. 1(b)) as it controls and sends commands to other ECUs, which acts as a gateway among different networks and can be compared to an Ethernet switch.

Besides, the dataflow viewpoint in Fig. 1(b) shows that the network Protocols are connected to their corresponding Dataflows, which regulate the communication between ECUs within the Networks, and also reflect that all messages from ECUs connected to the CAN Network are broadcast.

Furthermore, an Attacker is added to the Internet Network that connects with RADIO to make the threat model complete, with connection type "Compromise" (see in Fig. 1(a)), which indicates the entry point of this attack.

2015 Cadillac Escalade Model. Similarly, the 2015 Cadillac Escalade threat model is created according to its topology [17]. As is shown in Fig. 2, the network topology consists of three CAN Networks (i.e. PT-CAN, Low Speed GMLAN, and High Speed GMLAN), one LIN Network, and one MOST Network, where PT-CAN is the power train CAN protocol, and GMLAN is a CAN protocol for lower layer services.

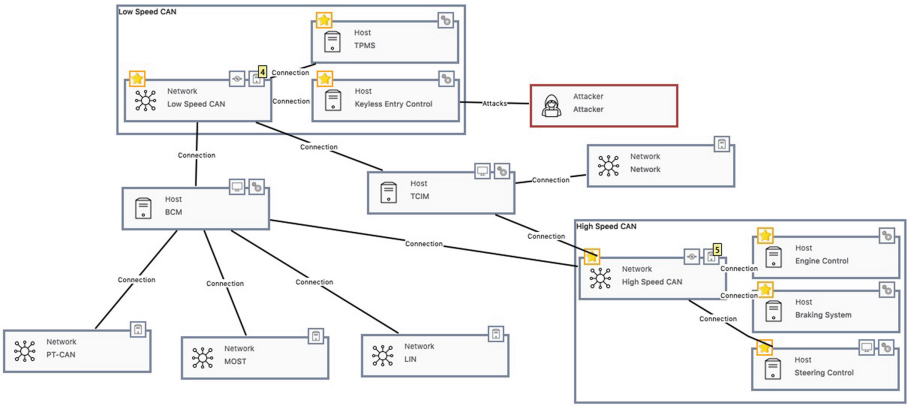


Fig. 2. 2015 Cadillac Escalade threat modeling.

The Low Speed CAN Network connects ECUs e.g. keyless entry control module, and telematics communication interface module (TCIM), etc. The High Speed CAN Network connects ECUs e.g. engine control module, braking system, steering control, etc.

Also, the Clients of both BCM and TCIM are connected to the low and high speed CAN Dataflows (not shown in the figure), because BCM includes ECUs e.g. steering control, pedals, and meters that need to send commands. Besides, we connect the Service of TCIM to both the Low Speed CAN Network and Dataflow (not shown in the figure), as TCIM contains a cellular connection required by the keyless entry control ECU within the Low Speed CAN Network.

Furthermore, we add an Attacker to the keyless entry control ECU, to simulate a scene where an attacker performs a keyless entry attack to gain unauthorized access and manipulate the vehicle. Note that an Attacker can be connected to other assets, modeling different entry points.

3.2 Security Settings

Based on the threat models we created, we assign security settings for each asset. This also includes the consequence for each attack, where the value ranges from 0 to 10 (with 10 being the most severe). Using the system model with security settings and the consequences of attacks securiCAD calculate quantitative measurements, e.g. risks according to the following equation:

$$Risk = Consequence \times Probability \tag{1}$$

As both the two vehicle models apply a SoftwareProduct called AUTOSAR, which also defines the function of the ECUs. Thus, we set the security settings for ECU and SoftwareProduct (i.e. AUTOSAR) of both the two threat models according to AUTOSAR classic documentation[10], and the reasons behind can be seen in Table 1 and Table 2, respectively.

A Network has countermeasures including DNSSec, PortSecurity and Static ARP Tables that are TCP/IP related. For the two CAN Networks, DNSSec settings are disabled. Both Services and Clients connected to ECUs have a countermeasure named Patched that is enabled.

Besides, a Protocol is connected to Dataflow, which gives options to choose different security implementations to apply on the communication over the networks, and the security measurements available are Authenticated, Encrypted and Nonce, where Authenticated is disabled from the security settings of CAN network Protocol[11].

[10] https://www.autosar.org/standards/classic-platform/.

[11] https://can-newsletter.org/uploads/media/raw/d904c90ba599c668e9758ae558dcb845.pdf.

Table 1. ECU security settings.

Defense	Description	Source for decision	Decision
ASLR	Address space layout randomization (ASLR) fortifies against buffer overflow attacks	Not implemented in AUTOSAR classic	Disabled
AntiMalware	It detects, removes and deters malware attacks	Not implemented	Disabled
DEP	Data Execution Prevention (DEP) defends against buffer overflow, by making memory areas non-executable	Not implemented in AUTOSAR classic	Disabled
Hardened	It represents the procedures where unused services, ports and hardware outlets are disabled	The open ports are found by Miller and Valasek in the radio box	Disabled for `RADIO` in Jeep model; enabled for other `ECU`s for both two models
HostFirewall	A firewall controls whether dataflow is blocked or allowed between hosts	No public information is available about how OEMs configure their firewalls	Unset
Patched	It means the host has the latest security updates	An Internet connection gives improved software support and patch availability	Patched with probability=50% for `BCM` in both two models; enabled for other `ECU`s
Properly Configured	It denotes that the asset is properly configured with regards to access control	No information available	Unset
Static ARP Tables	It means mapping IP address to MAC address to avoid spoofing	Only available for Ethernet	Disabled

2014 Jeep Cherokee Model. Here we assign the consequence for each attack under this model, and their underlying reasons. For example,

- Consequences of compromising Engine control, Transmission and Brake control `ECU`s are set to 10, because these `ECU`s are safety-critical, and the compromises of them could lead to fatal road accidents.
- Consequence of compromising `RADIO` is set to 3, as it is not so safety-critical.
- Consequence of a DoS attack on CAN-C `Network` is set to 9, because a DoS attack can shut down the access to `ECU`s of the network, and lead to fatal road accidents.

Table 2. SoftwareProduct security settings.

Defense	Description	Source for decision	Decision
HasVendor Support	Whether the software product is supported and has access to patches	The model has an Internet connection and is assumed to be supported	Enabled
NoPatchable Vulnerability	Whether the software product has no patchable vulnerabilities	No information available	Unset
NoUnPatchable Vulnerability	Whether the software product has no unpatchable vulnerabilities	No information available	Unset
SafeLanguages	The software product is developed in languages that perform checking to reduce the risk of buffer overflow	No information available	Unset
Scrutinized	Whether the software has been thoroughly tested and checked for vulnerabilities	No information available	Unset
SecretBinary	Whether there is an access to the binary by an attacker who can then detect vulnerabilities (no access to the binary makes it impossible to find new vulnerabilities)	No information available	Unset
SecretSource	Whether the source code is a secret source	AUTOSAR is an open-source	Disabled
StaticCode Analysis	Whether there is a code analysis tool to find vulnerabilities and bugs	No information available	Unset

– Consequence of a replay attack on CAN-C `Network` is set to 10, which represents the actual attack [18].

2015 Cadillac Escalade Model. Similarly, we assign consequences for attacks in the threat model. Since there is no public information showing the exact consequence value we instead provide arguments for our decisions. For example,

– Consequences of compromising Engine control, Braking system and Steering control `ECU`s are set to 10.
– Consequence of compromising `TCIM` is set to 3, as it is not so safety-critical.
– Consequence of a DoS attack on Low Speed CAN `Network` is set to 9, because a DoS attack can shut down the access to `ECU`s of the network, and lead to fatal road accidents.
– Consequence of compromising the keyless entry control `ECU` is set to 8, as it (in itself) should not lead to fatal road accidents compared to the former

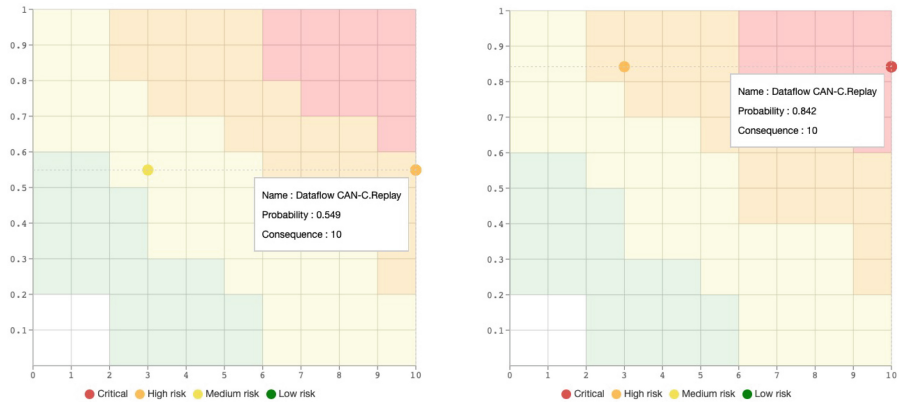
one. To prevent an attacker accessing the vehicle through compromising the keyless entry control `ECU` and then steal it, we can add `AccessControl` to the `ECU`, and see how it can change the attack path.

4 Vehicle Attack Simulations

After assigning the security settings to the created threat models, we are able to run the attack simulations. The simulation results include risk matrix, attack path, and Time to Compromise (TTC) graph, where the TTC graph presents the probability distribution based on a certain attack path of the expected time for an attacker to compromise an asset.

4.1 Risk Matrix

With the threat model and the security settings of the 2014 Jeep Cherokee Model, when we disable the `HostFirewall` of the `RADIO`, and the resulting risk matrix (shown in Fig. 3(a)) according to Equation (1) shows that the vehicle is not under critical risks. However, when the `HostFirewall` is disabled, the replay attack on CAN-C `Dataflow` is ranked Critical (shown in Fig. 3(b)), which reflects that the firewall is quite important to secure the network.



(a) Firewall enabled (b) Firewall disabled

Fig. 3. Risk matrix from simulations performed on the 2014 Jeep Cherokee model. [33].

Besides, if we change the security setting for `RADIO` from Disabled (see in Table 1) to Enabled, all possible attacks are ranked below Medium according to the simulation results.

4.2 Attack Path

The simulation results also show the attack path of an attack, which represent the possible composition of vulnerabilities used by an attacker. For the 2014 Jeep Cherokee Model, Fig. 4 indicates the attack path of the replay attack on CAN-C `Network`, where the unknown service indicates the D-bus service accessed in an actual attack [18], and they discovered that D-bus was running as root, which enabled them to get access to the vehicle remotely. Also, the green circle shows the countermeasures that could be implemented in this vehicle. We can see that most of the attack steps are related to `RADIO`, and we infer that the `Hardened` setting of `RADIO` is very important as it can be (is) the entry point for an attack. Besides, the width of the lines between attack (defense) steps indicates the likelihood of the attack path.

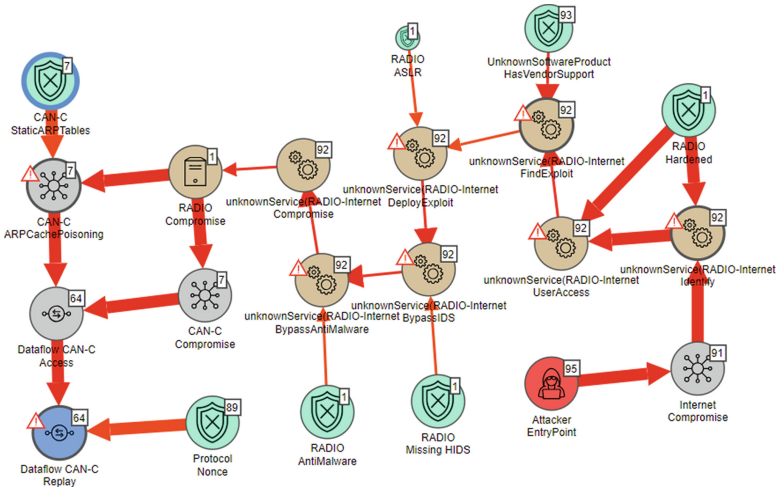


Fig. 4. Attack path of the Jeep replay attack. [33].

Similarly, with the threat model and the security settings, we can get the simulation results for the 2015 Cadillac Escalade Model. For example, the attack path of a keyless entry attack is shown in Fig. 5(a). If we add an `AccessControl` to the keyless entry control `ECU` it will be much more difficult for the attacker to compromise the keyless entry control `ECU` and steal the vehicle, the attack path for this can be seen in Fig. 5(b).

4.3 Time-To-Compromise (TTC)

TTC is used as a measurement of the effort for an attacker to conduct a successful attack. We assume that the attacker will take the shortest path, i.e. the least time-consuming way to the end node. The TTC of the replay attack on CAN-C

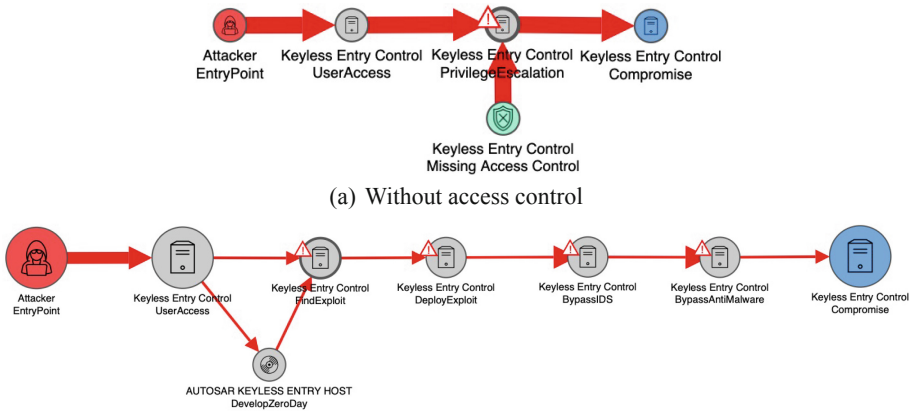


Fig. 5. Attack path of a keyless entry attack on Cadillac Escalade.

`Dataflow` can be seen in Fig. 6, which indicates how many days it takes to reach a certain probability of successfully compromising an asset. In this case, TTC for the replay attack to compromise the `Dataflow` is 20 days with a 50% probability, or is 10 days with a probability above 40%.

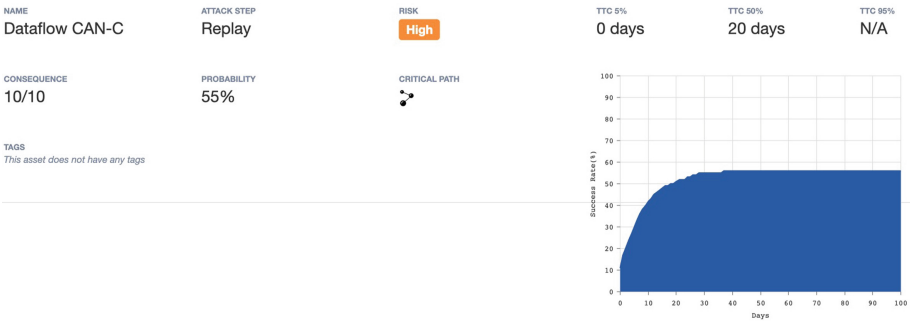


Fig. 6. TTC of a Jeep replay attack. [33].

Overall, the attack simulation results show that the modeled vehicles are not fully secure (as we also know from the real attacks we mimic). According to the risk matrix, we can infer the risk level of the vehicle. Also, we can change the security settings to see how it could influence the overall security level (e.g. Fig. 3). According to the attack path, we know what other countermeasures that can be implemented. At last, TTC provides a measurement of how secure the vehicle is in terms of attack resilience, which provides us a quantitative way of comparing vehicle architecture designs.

5 Discussion

In this paper, holistic threat modeling and quantitative attack simulations are conducted for the two most hackable vehicle models [17]-2014 Jeep Cherokee and 2015 Cadillac Escalade.

The simulation results works as a proof of concept of the approach. As creating large attack graphs for complicate systems manually is time-consuming and error-prone, this approach allows holistic identification and ranking of security-related threats that are likely to affect the vehicles. Also, the set of attack types and associated countermeasures (defenses) related to each asset in a vehicle could be explored and validated further. There are plenty of attacks known to the public for e.g. web applications and Windows-based systems, however, most of them might not be relevant for vehicles [4,28]. On the other hand, there might be certain attacks only related to vehicle systems. When it comes to countermeasures, a vehicle has certain limitations regarding performance, cost, and functionality that might not appear in other larger systems.

It appears that having a firewall is quite important to secure the vehicle [21]. Also, other assets e.g. the keyless entry control ECU can be entry points of attackers and therefore access control could be implemented as a countermeasure [1,2]. Therefore, designing network architectures is also important to vehicle security [9,29].

Furthermore, in order for the approach to be more efficient and for simulation results to be more useful, a metamodel that describes the fundamental assets and their associations of systems [8,15,22] needs to be tailored to fit the internal architecture of vehicles. Also, vehicle-specific statistical studies relating attacks and defenses quantitatively are still needed. This can be realized through hacking exercises or expert studies. Another important step is to validate and test the approach with case studies by modeling vehicles and iteratively enhancing the approach, similar work has been done in the energy domain [30]. Quantitative measures of security (e.g. TTC) require quantitative inputs in order to provide reasonable and useful output. Although it has been done for other system types, vehicle-specific statistical studies relating attacks and defenses are still need to be done.

6 Conclusion

This paper presents a proof of concept of an approach for connected vehicles using threat modeling coupled with attack simulations. Two vehicle models and publicly known attacks were modeled with a tool called securiCAD, showing that the approach is useful in its current state and allows holistic identification and ranking of vehicle security flaws, whereas a more vehicle-specific metamodel would be useful to describe the fundamental assets and associations of vehicles. Future work also includes studying vehicle-specific vulnerabilities, weaknesses, and countermeasures to provide more accurate attack simulation results.

Acknowledgment. This work has received funding from Vinnova, the Swedish Innovation Agency, and the FFI program.

References

1. Alrabady, A., Mahmud, S.: Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs. IEEE Trans. Veh. Technol. **54**(1), 41–50 (2005)
2. van de Beek, S., Leferink, F.: Vulnerability of remote keyless-entry systems against pulsed electromagnetic interference and possible improvements. IEEE Trans. Electromagn. Compat. **58**(4), 1259–1265 (2016)
3. Buttigieg, R., Farrugia, M., Meli, C.: Security issues in controller area networks in automobiles. In: 18th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering, pp. 1–6 (2017)
4. Checkoway, S., et al.: Comprehensive experimental analyses of automotive attack surfaces. In: USENIX Security Symposium, San Francisco, pp. 77–92 (2011)
5. Dakermandji, J.: An autosar diagnostic platform. Master's thesis, KTH Royal Institute of Technology, Stockholm, Sweden (2008)
6. Ekstedt, M., Johnson, P., Lagerstrom, R., Gorton, D., Nydrén, J., Shahzad, K.: Securi CAD by foreseeti: a CAD tool for enterprise cyber security management. In: 2015 IEEE 19th International Enterprise Distributed Object Computing Workshop (EDOCW), pp. 152–155. IEEE (2015)
7. Johnson, P., Lagerström, R., Ekstedt, M.: A meta language for threat modeling and attack simulations. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, p. 38. ACM (2018)
8. Johnson, P., Lagerström, R., Ekstedt, M., Österlind, M.: It Management with Enterprise Architecture. KTH, Stockholm (2014)
9. Johnson, P., Lagerström, R., Närman, P., Simonsson, M.: Extended influence diagrams for system quality analysis. J. Software **2**(3), 30–42 (2007)
10. Johnson, P., Vernotte, A., Ekstedt, M., Lagerström, R.: pwnPr3d: an attack-graph-driven probabilistic threat-modeling approach. In: Proceedings of the 11th International Conference on Availability, Reliability and Security, pp. 278–283. IEEE (2016)
11. Karahasanovic, A.: Automotive cyber security: threat modeling of the AUTOSAR standard. Master's thesis, University of Gothenburg, Gothenburg, Sweden (2016)
12. Karahasanovic, A., Kleberger, P., Almgren, M.: Adapting threat modeling methods for the automotive industry. In: Proceedings of the 15th ESCAR Conference, pp. 1–10. Chalmers Publication Library (2017)
13. Katsikeas, S., Johnson, P., Hacks, S., Lagerström, R.: Probabilistic modeling and simulation of vehicular cyber attacks: an application of the meta attack language. In: Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP) (2019)
14. Kordy, B., Mauw, S., Radomirović, S., Schweitzer, P.: Foundations of attack–defense trees. In: Degano, P., Etalle, S., Guttman, J. (eds.) FAST 2010. LNCS, vol. 6561, pp. 80–95. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-19751-2_6

15. Lagerström, R., Johnson, P., Höök, D.: Architecture analysis of enterprise systems modifiability-models, analysis, and validation. J. Syst. Softw. **83**(8), 1387–1403 (2010)
16. Ma, Z., Schmittner, C.: Threat modeling for automotive security analysis. Adv. Sci. Technol. Lett. **139**, 333–339 (2016)
17. Miller, C., Valasek, C.: A survey of remote automotive attack surfaces. In: BlackHat USA (2014)
18. Miller, C., Valasek, C.: Remote exploitation of an unaltered passenger vehicle. In: BlackHat USA (2015)
19. Ou, X., Boyer, W.F., McQueen, M.A.: A scalable approach to attack graph generation. In: Proceedings of the 13th ACM Conference on Computer and Communications Security, pp. 336–345. ACM (2006)
20. Park, J.S., Kim, D., Hong, S., Lee, H., Myeong, E.: Case study for defining security goals and requirements for automotive security parts using threat modeling. In: SAE Technical Paper. SAE International (2018). https://doi.org/10.4271/2018-01-0014
21. Pesé, M.D., Schmidt, K., Zweck, H.: Hardware/software co-design of an automotive embedded firewall. In: SAE Technical Paper. SAE International (2017)
22. Saat, J., Winter, R., Franke, U., Lagerstrom, R., Ekstedt, M.: Analysis of it/business alignment situations as a precondition for the design and engineering of situated it/business alignment solutions. In: 2011 44th Hawaii International Conference on System Sciences, pp. 1–9. IEEE (2011)
23. Saini, V., Duan, Q., Paruchuri, V.: Threat modeling using attack trees. J. Comput. Sci. Coll. **23**(4), 124–131 (2008)
24. Salfer, M., Eckert, C.: Attack graph-based assessment of exploitability risks in automotive on-board networks. In: Proceedings of the 13th International Conference on Availability, Reliability and Security, pp. 1–10. ACM (2018)
25. Salter, C., Saydjari, O.S.S., Schneier, B., Wallner, J.: Toward a secure system engineering methodology. In: Proceedings of the 1998 Workshop on New Security Paradigms, pp. 2–10. ACM (1998)
26. Shostack, A.: Threat Modeling: Designing for Security. Wiley, Indianapolis (2014)
27. Sion, L., Van Landuyt, D., Yskout, K., Joosen, W.: Sparta: security & privacy architecture through risk-driven threat assessment. In: 2018 IEEE International Conference on Software Architecture Companion (ICSA-C), pp. 1–4. IEEE (2018)
28. Välja, M., Korman, M., Lagerström, R.: A study on software vulnerabilities and weaknesses of embedded systems in power networks. In: Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids, pp. 47–52. ACM (2017)
29. Van Bulck, J., Mühlberg, T., Piessens, F.: Vulcan: efficient component authentication and software isolation for automotive control networks. In: ACM International Conference Proceeding Series, pp. 225–237 (2017)
30. Vernotte, A., Välja, M., Korman, M., Björkman, G., Ekstedt, M., Lagerström, R.: Load balancing of renewable energy: a cyber security analysis. Energy Inform. **1**(1), 1–41 (2018). https://doi.org/10.1186/s42162-018-0010-x
31. Williams, I., Yuan, X.: Evaluating the effectiveness of microsoft threat modeling tool. In: Proceedings of the 2015 Information Security Curriculum Development Conference, p. 9. ACM (2015)
32. Xiong, W., Gülsever, M., Kaya, K.M., Lagerström, R.: A study of security vulnerabilities and software weaknesses in vehicles. In: Askarov, A., Hansen, R.R., Rafnsson, W. (eds.) NordSec 2019. LNCS, vol. 11875, pp. 204–218. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-35055-0_13

33. Xiong, W., Krantz, F., Lagerström, R.: Threat modeling and attack simulations of connected vehicles: a research outlook. In: Proceedings of the 5th International Conference on Information Systems Security and Privacy (ICISSP) (2019)
34. Xiong, W., Lagerström, R.: Threat modeling - a systematic literature review. Comput. Secur. **84**, 53–69 (2019)
35. Xiong, W., Lagerström, R.: Threat modeling of connected vehicles: a privacy analysis and extension of vehiclelang. In: International Conference on Cyber Incident Response, Coordination, Containment & Control (Cyber Incident). IEEE (2019)