Incident Response for Vehicular Systems – More than online Updates

Falk Langer[1][0000-0001-8780-0868] and Fabian Schüppel[2][0000-0003-4218-6459]
and Lukas Stahlbock[3][0000-0002-4426-103X]

[1,2,3] IAV GmbH, Berlin, Germany

Abstract. Cybersecurity incidence response is an important building block for the safe operation of vehicles over their lifetime. The systems in need of protection within the vehicle are vulnerable to attacks over the internet. The strict safety requirements, complexity and large number of vehicle variants on the other hand lead to the issue, that in the case of a discovered vulnerability, developing an update fixing said vulnerability will take a long time – most likely making damage by attacks a certainty.

Within this paper, we show mechanisms to speed up the incidence response. For this reason two new levels of responses are proposed, which allow a reaction within minutes without impairing the requirement of safe and reliable operation.

Keywords: security, vehicle, automotive, incident response, secure operation, safe mode, OTA, cyber defense center, security management, security monitoring.

1 Introduction and Motivation

Today’s vehicles have already different online connections: For instance, infotainment systems often include navigation with real time traffic, online maps, smartphone connections, as well as audio- and video streaming. Besides these non-security-critical connections, modern high-class cars are using online connection for unlocking, summoning or updating the car. To prevent drivers and environment from the risk of cyber-attacks as shown in the well-known jeep hack, United Nations (UN), ISO/SAE and the NHTSA, are increasing their focus on vehicle cyber-security, which indicates that it is not only important for product quality from OEMs, but rather for well-being of humans. As a result the “UN Task Force on Cyber security and OTA issues (CS / OTA)” [6] defines a cyber-security management and monitoring system with incident response as a necessary part of a cybersecurity system.

This results in the need for an Automotive Cyber Defense Center (ACDC) [4], which is responsible for secure operation of their cars. The most important building blocks of an ACDC are Security-Sensors within the cars, a security information and event management (SIEM), a security operation center (SOC) and the incident response. First

OEMs [3] and TIER1 [1] supplier have presented cyber-security systems with intrusion detection systems.

Within this paper, we focus on the incident response for operation of vehicle fleets. In IT-Systems for this topic, there exists security incidence response teams [5]. One of the major activities of these SIRT is the planning and enrolling of the reaction to an incidence. These reactions are mostly (i) reconfiguration of firewalls, proxies, forwarding rules etc. pp., (ii) deactivating of services and (iii) applying patches.

It may be obvious, that such kind of changes within a complex IT System need to be planned and executed carefully to not cause any collateral damage. Subsequently the response by an automotive SIRT within a fleet of millions of different vehicles seems to be a challenging topic. Within this paper, we like to discuss basic concepts and techniques for applying a security response to a vehicle fleet. With respect to the safety critical applications, the inhomogeneous character of cars internal IT infrastructure and the long period of maintenance the existing response strategies known from e.g. data centers or mobile phones need to be adapted or enhanced.

2 Requirements for an automotive incident response mechanism

The US National Institute of Standards and Technology defines in the Computer Security Incident Handling Guide (SP 800-61) [7] four phases of incident handling. These are

1. Preparation
2. Detection and Analysis
3. Containment, Eradication and Recovery
4. Post-Incident Activity.

These phases are certainly applicable for the incident response (IR) for a vehicle fleet but the content and the responsibility need to be redefined.

One of the boundary conditions is that an update of security measures on vehicle level has consequences on fulfilling safety and legal requirements on a vehicle [1]. Subsequently any changes on behavior at vehicle level are equivalent to a software update. That means that there will be different planning loops according to the Handling Guide. At least one for measurements within the vehicle and one for measurements on backend side.

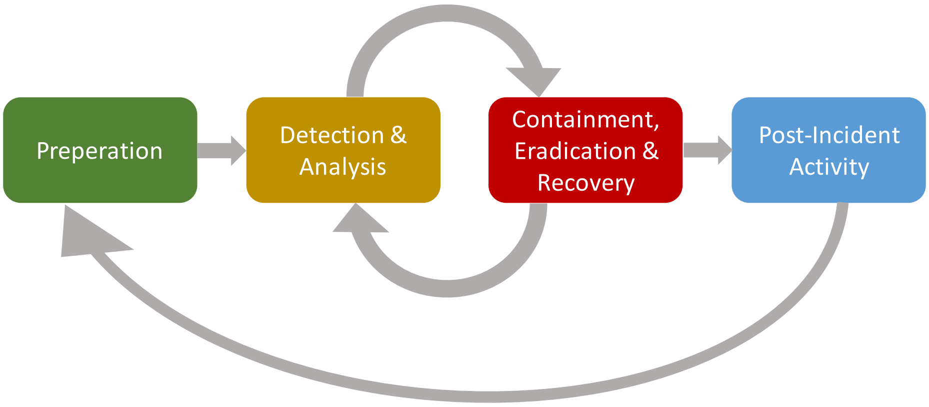

Fig. 1. Incident response life cycle as described by NIST [7]

In the following, we concentrate on the inner cycle of the planning loop. That is "(2) Detection and Analysis" and "(3) Containment, Eradication and Recovery". More specific we propose possible technics beside an ordinary software update. We expect to have more and faster mechanism to response to an incidence that limits and reduces possible impacts to vehicles.

3 Potential stages for Responses

The response loop for backend server applications might be a well-known task. However, what about the response for services or software running inside the vehicles? Mostly the response for Internet of Things / IoT applications is described as a software update (Over The Air update / OTA). Nevertheless, the creation of a software update for vehicles and its roll out is complex and takes some time. We estimate the creation and roll out of software updates because of vulnerability in the range of months, may be some weeks. However, this time seems to be too long for reacting on incidents in comparison to the remaining IT-Industry.

We assume that it should be possible to give first responses on incidents in the range of minutes or hours. Nevertheless, it is also clear that within this short time range there could be no complex systematic answers. For this reason, we propose to have different response levels (**Fig. 2**).

1. Level – Immediate response: Containment of attacks and risk limitation for individual vehicles
2. Level – Intermediate response: Recovery of system behavior by isolating or deactivating affected services, reconfiguration of network and security rules
3. Level – Long-term response: Eradication of vulnerabilities, Bug fixes to prevent future attacks

New in this context for vehicular applications are the first and second level. These levels are introduced to reduce the response time for incidents. To achieve the goal of faster response with concurrent need for stable and safe operation of vehicles the validation and execution of measures need to be adjusted.

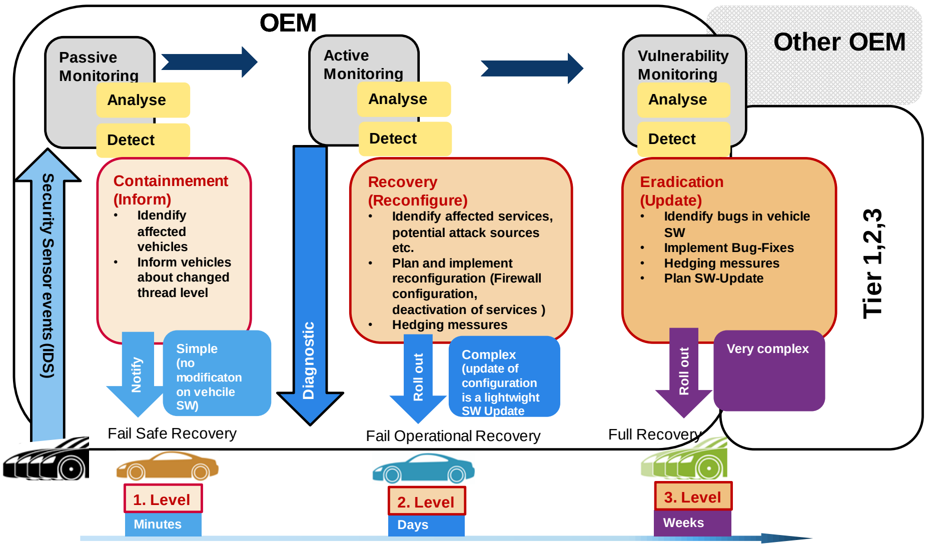
OEM
Other OEM
Passive Monitoring
Analyse
Detect
Active Monitoring
Analyse
Detect
Vulnerability Monitoring
Analyse
Detect
Security Sensor events (IDS)
Containmement (Inform)
• Idendify affected vehicles
• Inform vehicles about changed thread level
Notify
Simple (no modificaton on vehcile SW)
Diagnostic
Recovery (Reconfigure)
• Idendify affected services, potential attack sources etc.
• Plan and implement reconfiguration (Firewall configuration, deactivation of services)
• Hedging messures
Roll out
Complex (update of configuration is a lightwight SW Update
Eradication (Update)
• Idendify bugs in vehicle SW
• Implement Bug-Fixes
• Hedging messures
• Plan SW-Update
Roll out
Very complex
Tier 1,2,3
Fail Safe Recovery
Fail Operational Recovery
Full Recovery
1. Level
Minutes
2. Level
Days
3. Level
Weeks

Fig. 2. Three levels of response: Containment, Recovery and Eradication

3.1 First Level

For the first level, we propose to inform the vehicles about an observed threat level and let itself decide how to deal with this information. In this case, the planning of any reaction will be done in the development phase of the vehicle. We assume that it is possible to set some safe fallback states that a vehicle can go for different threat levels. May be untrusted services are disabled, feature updates are postponed or services with external communication paths are disabled.

The vehicle fleet is monitored passively in this case. That means only data or events from the vehicles that are provided by default will be used for observation.

We assume that this notification to vehicles can be at least prepared full or semi automatically or on a defense center depending on the notified threat level and the number of informed vehicles. However, since there are no changes in the vehicular system the stability and safety of vehicle functionality is not effected. In conclusion, these responses can be sent within seconds after detection of possible attacks.

3.2 Second Level

In contrast to first level, we propose for second level to not only inform the vehicles about an observed threat but also pass some new system configuration. From the log analysis, one can identify which services or system element (e.g. which ECUs) may be affected. The new configuration shall than only deactivate the affected services or isolate a system element. This provides more flexibility than first level actions and less time than third level actions. Looking into the E/E-architecture development trends for upcoming vehicle generations we can describe one example realization of a second level response. Modern vehicles will have vehicle centric E/E-architectures with a domain or zone-based grouping of embedded ECUs [8][9]. The most computational power will be concentrated in the vehicle centric computing unit. By introducing a high-availability cluster of several ECUs instead of a single computing unit a more flexible service orchestration is possible. In automotive systems, the AUTOSAR Adaptive Platform for example, uses a service-oriented architecture and allows dynamic service discovery [10]. This can be utilized to orchestrate services in several ways depending on the operation mode of the vehicle [11]. One scenario for second level response could be to dynamical reconfigure the orchestration mode. This aims to provide driving ability along with as much other functionalities as possible. The incident response team needs to determine possible weak spots from the security sensor events. Based on these they can create restrictions for the service orchestration that are passed to vehicle orchestrators. Potentially insecure services are deactivated and other services are isolated in a trusted environment. Therefore, services in the vehicle centric computing unit shall not be bound to a specific hardware but should be portable across several ECUs. This can be achieved by creating containerized applications for each service and using a cluster as a computing platform. To use container in a mixed criticality system such as the automotive domain, is only possible with the support from the operating system [12]. The most popular open source cluster framework is Kubernetes which has a lightweight implementation that is viable for embedded devices such as automotive ECUs [13]. Kubernetes provides the possibility to create a customized scheduler that starts and stops applications and assigns them to ECUs. A second level response of this kind depends on such a configurable scheduler.

4 Discussion and Outlook

Within this paper, the problem of incidence response to vehicles is discussed. The currently commonly promoted response in form of software updates takes too much time and is complex in planning, creation and roll out. To overcome these limitations two new level of response are proposed to make a response faster, scalable and easier to handle.

We think that for both new levels –Information and Reconfiguration- there exists methodologies within the vehicle software that can support such kind of response. The given examples include the switch between different vehicle states with different behavior. In addition, the partial deactivation of services is used e.g. for obtaining additional time for a long-term solution. It needs to be emphasized, that an interaction with manufacture backends is commonly new for vehicles.

We try to give an impulse to think more about incidence response in the planning phase of connected vehicle software architectures. The methods, technics and tools are available and just need to be included within future architectures.

References

1. VERORDNUNGEN VERORDNUNG (EU) 2019/2144 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. November 2019, https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32019R2144&from=DE
2. Cyber-Sicherheitslösungen von Argus und Elektrobit für die vernetzte Fahrzeugelektronik von Continental, Pressemeldung Continental 24.07.2018, https://www.continental.com/de/presse/pressemitteilungen/2018-07-24-cyber-security-137176
3. VW ID.3: 3 Hochleistungs-PCs und Microsoft-Azure-Cloud, Hans-Christian Dirscherl 11.09.2019 https://www.pcwelt.de/news/VW-ID.3-3-Hochleistungs-PCs-und-Microsoft-Azure-Cloud-10664687.html
4. Establishing an Automotive Cyber Defense Center, Falk Langer, Fabian Schüppel, Lukas Stahlbock, In: 17th escar Europe : embedded security in cars, 2019
5. Defining Computer Security Incident Response Teams, Robin Ruefle, https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams, 24.1.2007
6. UN Task Force on Cyber security and OTA issues (CS/OTA) https://wiki.unece.org/download/attachments/81888965/TFCS-TPahCS2-04%20Draft%20Recommendation%20on%20Cyber%20Security%20-%20capturing%20suggested%20amendments%20from%20test%20phase%20participants.docx?api=v2, last accessed 2019/06/12
7. US National Institute of Standards and Technology defines within Computer Security Incident Handling Guide (SP 800-61) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
8. Functional architecture and E/E-Architecture – A challenge for the automotive industry, D. Zerfowski, A. Lock, Proceeding of 19. Internationales Stuttgarter Symposium, 2019
9. Serviceorientierte EE-Zonenarchitektur Schlüsselelement für neue Marktsegmente, M. Maul, G. Becker, U. Bernhard, ATZ elektronik 01/2018
10. Explanation of Adaptive Platform Design, https://www.autosar.org/fileadmin/user_upload/standards/adaptive/19-11/AUTOSAR_EXP_PlatformDesign.pdf
11. A Dynamic Service-Oriented Software Architecture for Highly Automated Vehicles, A. Kampmann, B. Alrifaee, M. Kohout, A. Wüstenberg, T. Woopen, M. Nolte, L. Eckstein, S. Kowalewski, IEEE Intelligent Transportation Systems Conference (ITSC), 2019
12. RT-CASEs: Container-Based Virtualization for Temporally Seperated Mixed-Criticality Task Sets, M. Cinque, R. Corte, A. Eliso, A. Pecchio, 31st Euromicro Conference on Real-Time Systems (ECRTS 2019), pp. 5:1 – 5:22
13. Adapting a Container Infrastructure for Autonomous Vehicle Development, Y. Wang, Q. Bao, arXiv:1911.01075v2, 19.11.2019