WANNADRIVE?

Feasible Attack Paths and Effective Protection Against Ransomware in Modern Vehicles

Marko Wolf, Robert Lambert⋆, Aubrey-Derrick Schmidt*, and Thomas Enderle**
**)ESCRYPT GmbH – Embedded Security, ⋆)ETAS Embedded Systems Canada Inc.*

Abstract: Ransomware on vehicles has the potential to become a real threat to vehicles for the same reason that it has become a significant and persistent menace to IT infrastructure in institutions and businesses: there is a compelling business model behind. Victims of ransomware on vehicles will also have compelling reasons to pay the ransom demanded to regain access to their vehicles, or to restore their vehicles to a properly functioning state. We assume, this would be particularly relevant for commercial vehicles, public vehicles, and for large vehicle fleet owners, since they often serve critical and urgent tasks with high damage potentials and since they have the financial power to pay even high ransoms.

With this article, we will explain how ransomware might be used to attack vehicles and extort drivers and vehicle owners. We will demonstrate that vehicle ransomware can be readily created and deployed, showing that that threat of ransomware on vehicles is real and present. In fact, we believe, that with the growth and importance of interconnected information technology in vehicles together with its continuous standardization, the security threat through ransomware will become even larger.

Hence, we will also give several practical recommendations for preparing ahead against the ransomware threat with holistic multilayered protections, but also extending vehicles and vehicle organizations with the ability to react on potential ransomware attacks with updated defenses and responses.

Keywords: Ransomware, automotive security, cyber security threat, connected vehicle

1 Introduction

Since the recent, prominent attacks of *CryptoLocker*, *WannaCry*, and *Petya* against several critical IT systems, ransomware, which means any kind of cyber extortion malware, has become very popular topic heavily discussed in industry, academia, and the media. Today's ransomware effectively capitalizes on the increasing digitalization and connectivity of virtually every area in our life, together with our increasing dependence on such interconnected IT systems. Ransomware has already successfully infected personal computers, public and private enterprise IT systems, websites, smartphones, industrial control systems, and even live TV stations. However, one very prominent connected device used every day by billions of people has not been affected yet – the modern connected vehicle.

Hence this work will provide a deeper look at possible attack scenarios, possible attack paths, and especially on effective protections against ransomware in vehicles.

Critical Vehicle Security Attacks Are Still Rare in Real Life

Since modern vehicles have become increasingly software-driven, connected, and complex, they have also become increasingly susceptible to new cyber security attacks. Increasing software deployment widens the number of potential attack targets, increasing connectivity widens the potential attack surface, and growing complexity increases the chance for an exploitable security vulnerability. On one hand, virtually all known vehicle security attack patterns have already been successfully demonstrated in practice, including remote cyber security attacks on safety-critical driving functionality, such as vehicle steering and braking [1]. On the other hand, except for some prominent alertness attacks such as [3] and [4], critical vehicle security attacks with a real safety impact, that is, attacks which effect the safety of driving the vehicle (a *driving safety attack*) are not (yet) a real-life issue. Hence, the most common vehicle security attacks today are unchanged from yesterday, meaning vehicle (component) theft, odometer manipulation, (chip) tuning, and counterfeit part production.

Serious Cyber Security Attacks Do Scale to Significant Profits

To our understanding, there are at least two reasons that safety attacks have not yet developed. First, creating a driving safety attack requires a lot of time and money (i.e., many person months and >100 k$), but yields an attack which is applicable only on a certain type or class of vehicle. Attacks are not typically easily transferable from one vehicle to another due to the heterogeneity of most vehicular onboard IT architectures and software. Second, successful driving safety attackers are, up to now, rewarded only with some (academic) fame but no real financial gain for the attackers. However, looking at other IT domains (e.g., business IT), the most successful attacks are exactly those which do (i) easily scale and (ii) have a "business model" that works, such as software piracy, phishing, and ransomware. Could these attacks also become serious security threats for modern vehicles? Software piracy and the physical equivalent: theft, are serious, but currently well-known and at least already tackled security threats within the automotive domain (cf. various more or less effective anti-theft and anti-counterfeit mechanisms). Phishing in turn usually tries to exploit careless behavior which people from time to time will exhibit when interacting with their applications or devices. However, vehicular IT usually has to be highly automated without many direct user interactions such as password entry, which could be attacked by social engineering attacks. Ransomware, however, has not really been tackled by automotive security engineers yet. However, this could change quickly.

Ransomware is Already a Very Successful Security Threat in Business IT

Ransomware, by which we mean any kind of cyber-extortion malware, has already been proven to be very successful and lucrative in real life (cf. [9], [10], [11]) particularly since the most critical challenge of such extortion: anonymous payment, has been solved using reliable, easy to use cryptographic currency such as Bitcoin. According to recent studies such as [15] and [16], the global ransomware infection ratio in unsolicited emails is up to 70% with more than 40% of victims actually paying the demanded fee, which is typically between $200 and $10,000. Cyber criminals have already extorted roughly $1 billion in 2016. Assuming that only 10% of the 250 million connected vehicles in 2020 (according to Gartner Inc.) are susceptible to ransomware attacks, and that 20% of victims are willing to pay a ransom of $200, then the potential "attack market" is already more than one billion dollars (likely a conservative estimate). Hence, there seems at least a reasonable financial motivation for blackmailing connected vehicles or vehicle fleet owners.

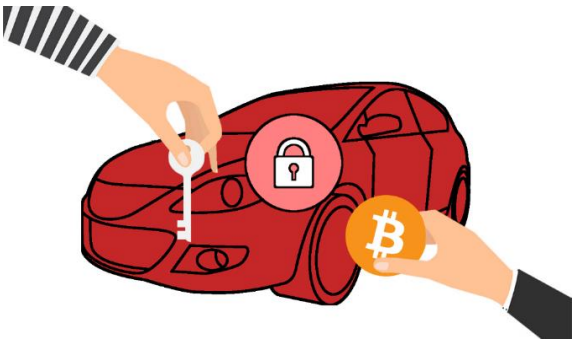

Figure 1: In near future, ransomware against all kind of vehicles could become a realistic and serious security threat.

2 Vehicular Ransomware Attack Scheme

This section describes the prerequisites and the procedure for executing a vehicular ransomware attack.

Vehicle Ransomware Attack Prerequisites

In order to execute a vehicular ransomware attack, the cyber-criminal would need at least the following:

a) A *ransomware malware* client and server software for on-board realization of cyber extortion on the target vehicle along with corresponding remote control.
b) An *anonymous botnet* for global distribution and remote control of the ransomware vehicle clients.
c) An *in-vehicle security exploit* usually together with Trojan software for reaching and infecting a connected in-vehicle unit in order to install and execute the ransomware malware client.
d) An *on-board lock* or *bricking action* for a critical vehicle component which cannot (easily) be restored, circumvented, or that cannot afford a long failure duration; ideally combined with a (secret) unlocking command to release the locked vehicle component once the ransom has been paid.
e) An *anonymous payment scheme* to receive the ransom and to protect the blackmailer against exposure and subsequent legal action.

Vehicle Ransomware Attack Scheme
Based on these prerequisites, and as shown Figure 2, a typical ransomware attack scheme could be the following.

The cyber-criminal (3) creates (a) and distributes (c) its ransom malware (2) to its extortion target vehicles (11) using ransom control software (5, "bot master") behind an anonymous botnet (4) applying for instance TOR technology [32]. The criminal might then try (b) to inject the ransomware directly (c2) or indirectly (c1, via a secondary security exploit) over any wireless (6a) or wired interface (6b) that might reach the target vehicles. Once the malware reaches a potential target vehicle, it uses the integrated vehicle primary security exploit (d) to install and execute the ransomware client (8) at a central, well-connected in-vehicle unit (7) such as the infotainment unit misusing it has host for its further actions. From there, the ransomware client might either first create an online connection back to the blackmailer in order to receive further data ("pay load") and/or further commands (e), or it might directly communicate (f) to a critical target ECU such as ignition control (10) via in-vehicle bus systems (9a) to execute the actual onboard *locking action* (g) in order to extort payment from the ransom victim (12). Now the ransomware would display its extortion message (h) and demand payment of the corresponding ransom. After the victim has paid the ransom (i) using an anonymous payment scheme (13) such as Bitcoin, the blackmailer would contact its ransomware again using its anonymous botnet (e2) to execute the necessary (secret) *unlocking command* (f) to release the vehicle (if possible).

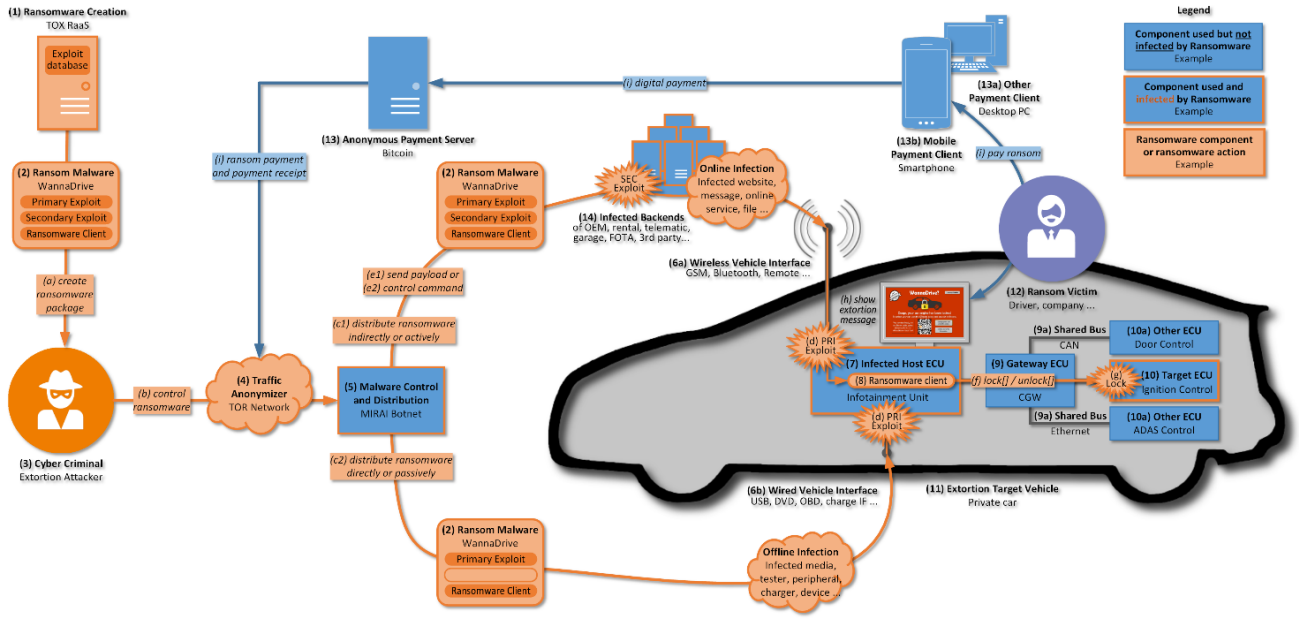

Figure 2: Vehicle ransomware attack scheme where a cyber-criminal (3) attacks a vehicle (11) to extort its victim (12).

3 Vehicular Ransomware Attack in Practice

In the following section, we give an overview on how the theoretical approach for a vehicular ransomware, as presented in Section 2, could be realized in practice. However, until now there are no real-life vehicular ransomware examples known to the authors except some (rather unsuccessful) vehicle-related cyber extortions attempts for instance by attacking a connected vehicle smartphone application [23], but never the vehicle itself.

3.1 Creation of a Vehicular Ransomware Malware

Cyber-criminals who want to use ransomware software do not have to program the required malware by themselves. There already exist several ready-to-use ransomware construction kits or ransomware-as-a-service (RaaS) offers, such as TOX [19] or STAMPADO [31]. These kits include the necessary malware control server ("bot master") and ready-to-use interfaces to an anonymous payment scheme like Bitcoin and to traffic anonymizers like TOR. Even though today's ransomware kits target mainly Microsoft Windows runtime environments, we believe it is only a matter of time, or better, a matter of "(financial) attractiveness", that such ransomware kits will also provide automatic creation of ransomware for automotive Linux or even AUTOSAR OS environments. The increasing application of Linux and AUTOSAR within modern vehicles, and the ongoing homogenization, modularization, and standardization of vehicle software will considerably enlarge and

uniformize the attack surface, making vehicle (ransom) malware distribution and execution much more efficient and scalable.

Usually such ransomware kits also provide some common security exploits for the ransomware distribution (secondary exploit) and target infection (primary exploit) or enable the cyber-criminal to provide individual, much more powerful undisclosed (so-called "zero day") exploits to be supplied for integration into the ransomware software (cf. Section 3.3 for further vehicle-specific details). Next, the cyber-criminal has to choose the target-specific "extortion mechanism" like data encryption, component locking, or any other kind of unwanted behavior targeting the extortion target which fill force the victim to pay the demanded ransom (cf. Section 3.4 for further vehicle-specific details).

As a last step, the ransomware kit automatically creates a complete ransomware software package including the ransomware target client, the primary and secondary security exploits (if possible), and the actual extortion mechanism together with the necessary ransomware remote control facilities ("bot master").

3.2 Distribution of Vehicular Ransomware Malware

For efficient, large-scale, and anonymous distribution of the ransomware, the cyber-criminal would use or hire a TOR-based botnet such as MIREI [20] which provides more than 400.000 "bot clients" starting from $ 1.000 per week [21]. While today's botnets do not directly reach vehicles, they can at least indirectly infect vehicles by infecting and misusing a host system that has a digital communication channel to the vehicle. These host systems or communication channels could be:

- Websites retrieved by the vehicle (e.g., drive-by-downloads accessed through the on-board infotainment unit or through hidden machine-to-machine website requests)
- Messages retrieved and interpreted by the vehicle[1] (e.g., emails, SMS, digital messengers, e-call, DAB+ radio, television [25])
- Personal devices connected to the vehicle (e.g., smartphones, digital memory, navigation, OBD plugins)
- Any OEM or supplier backend connected to the vehicle (e.g., for FOTA updates, remote diagnosis, cloud services)
- Any 3rd party backend connected to the vehicle (e.g., for insurance, telematics, toll, logistics, leasing)
- Any 3rd party device connected to the vehicle (e.g., trailers, vehicle peripheral or attachments, electric charging station, garage devices, digital tachograph)
- Traffic infrastructures (e.g., traffic management systems, site access control devices, toll systems, V2X)

Depending on the power of our ransomware construction kit (cf. Section 3.1), our ransomware might include its own secondary infection mechanism, which could then be used by the ransomware to actively distribute itself (e.g., like a computer worm). If not, the ransomware has to rely on passive distribution by the infection mechanisms provided by the corresponding botnet in order to reach the susceptible vehicle interfaces. Once the ransomware has successfully been deployed on a host system which has a digital communication channel to a susceptible vehicle interface, it would then use its primary infection routine the get into the vehicle, as described in the next Section 3.3.

3.3 Infecting the Target Vehicle

Once the ransomware has reached one of the various digital vehicle interfaces, it would use its primary security exploit to install and execute the malicious ransomware client on a sufficiently powerful and well-connected in-vehicle electronic control unit (ECU) such as the infotainment unit or the central communication unit. As recent studies such as [1], or prominent incidents such as [3] have shown, there already exits several in-vehicle security vulnerabilities that could have been misused by ransomware, including:

- USB port vulnerability at vehicle infotainment system [5]
- OBD port vulnerabilities to access all in-vehicle busses [2]
- CD/DVD player vulnerability at vehicle infotainment system [1], [6]
- Bluetooth buffer overflow vulnerability at vehicle infotainment unit [1]
- Cellular vulnerability at central vehicle communication unit [3], [1]

[1] Additional assumption by the authors: there will be lists of user email addresses / ID handles used by industry / advertisers to specifically address drivers. These lists will get lost sooner or later, as the past years mass data leaks have shown [24].

- Wi-Fi vulnerability at electric vehicle charging system [4]
- Remote vulnerability at aftermarket telematics control unit (TCU) [7]
- Vehicle mobile app vulnerabilities to access vehicle internals [8]
- Wi-Fi stack exploitation by Google Project Zero [26], [27], [28]

The further increasing vehicle digitalization, increasing vehicle networking, and especially the increasing vehicle IT homogenization and standardization will again "help" a lot to increase the scalability of the attack i.e. wide-spread uniform vehicular security vulnerabilities that could be misused by vehicular ransomware to infect the vehicle. A first outlook on the impact of this is given in in [26], [27], [28]. A Google Project Zero member [29] found a flaw in a popular Broadcom Wi-Fi chip/firmware built into some Google Nexus phones, but this chip is also used in several others popular devices, e.g. also Apple iPhones. Apple closed this vulnerability within days [26], realizing the severity of this finding and the importance of a proper patching plan and corresponding infrastructure. A lot of other companies might not react this quickly, ending up with a large number of vulnerable devices and vehicles.

Since there is only a very limited number of chip producers, the population of affected devices in such cases is pretty large, typically "millions of devices", and depending on the reuse of affected code, firmware and drivers, the number might be much higher. Additionally, it can be expected that exploits effective against a wide number of vehicles will sooner or later be sold, since the value of such exploits is obvious, and also because holding a locked or disabled vehicle hostage can reasonably be expected to severely affect the victim, leading to higher rates of paid ransoms.

3.4 Extortion at the Target Vehicle

Once the ransomware client has been successfully installed and executed within the vehicle, it will undertake the actual hostage-taking. For vehicles, the hostage could be for instance (i) a locked or "bricked" critical in-vehicle component, which cannot (easily) restored, circumvented, or that cannot afford a long failure duration or (ii) seizing or leaking of critical in-vehicle data, which cannot (easily) restored or that would result in a considerable damage if it would become publicly available, or (iii) anything else in order to force the victim to pay the ransom. In some cases, merely maliciously claiming to have something locked or become leaked (also known as *scareware*) could already be sufficient to effectively extort the victim. Some exemplary bricking, locking or leaking in-vehicle extortion actions could be for instance:

- Setting an important ECU (e.g., engine control, crop function, door lock) into firmware update, diagnosis, or similar maintenance mode via corresponding UDS command, blocking the actual ECU functionality. This attack is very simple and effective (cf. Hackers Handbook [22] for further explicit UDS or CAN bus commands).
- Locking important cryptographic credentials (e.g., keys, certificates) that cannot easily recovered and through this means preventing, for instance, ECU authentications, V2X communication, remote door locks, vehicle platooning, trailer/peripheral connection, or any other kind of cryptography-based vehicle functionality.
- Encryption of critical in-vehicle data such as a personal media repository, personal communication, or relevant logs (within a private car) or electronic routes, freight documents, legally relevant driver logs, customer required freight monitoring logs, important control parameters/data for steering integrated peripherals or attachments like concrete mixers or harvesters (within commercial vehicles).
- Leaking critical in-vehicle data such as speed limit or traffic violations, illegal media downloads, illegal routes to real or fictitious authorities (e.g., highway police). As an example, ransomware sometimes offers to prevent a later large fine if a smaller fine is paid now.
- Leaking critical in-vehicle data such as freight data, routes, farm/crop data, dash camera videos (of incidents or accidents) to concurrency or other critical platforms (from the victim's perspective).
- Scaring the victim with technical or problems such as expired licenses, expired leases, expired activations, or any other critical technical conditions (e.g., an overheated battery or transmission).
- Real physical manipulation or destruction of critical components (e.g., concrete pump in a commercial car, load control at tank truck, freight temperature control manipulation, air condition in coach, short-circuit the battery, trigger all airbags, or try to kill the engine using a destructive engine control signals).
- Manipulation of sensor or servo data in industrial vehicles, e.g. disabling geo-fencing of harvesters.

Another very promising ransomware attack target is the more and more prominent automotive hardware security modules (HSM) such as SHE [17]. Originally intended to improve security, they can also become targets of ransomware, which directly attacks the HSM security functions and responses. Ransomware could for instance misuse the secure boot mechanism with a dedicated software manipulation in order to prevent the usage for critical cryptographic keys bound to a certain boot configuration. To the authors' knowledge, HSM-based security architectures do not consider such Denial-of-Service attacks.

It is already apparent that commercial and public vehicles are more promising ransom victims than are private cars. In many cases, private drivers would have no absolute urgency and would call the garage or use a taxi instead of paying the ransom. And even if they are willing to pay the ransom, private drivers would accept only relatively small ransom payments and could often also fail to use or not already be setup to employ complex anonymous payment schemes as Bitcoin. Whereas, commercial or public vehicles and large vehicle fleet owners are much more promising ransom victims especially for instance:

- trucks with their tight schedules, sensitive goods, and severe contract penalties,
- coaches with their similar tight schedules transporting up to 70 passengers in a hurry,
- agriculture machinery which cost millions $ while being used only some weeks per year in the field,
- construction vehicles or any other special vehicles with complex, expensive, and dangerous equipment,
- public authority vehicles critical for public safety and security such as police, fire department, or hospital vehicles,
- car rental or car leasing companies, but also large company-owned vehicle fleets or even OEMs,
- and last but not least even military vehicles.

Vehicular ransomware for the above targets would be a much more attractive, since these victims have a high urgency to re-active their functionality since they are often serving critical tasks. They are also then more likely to pay the ransom payment and have the financial power to pay much higher ransoms, while also being able to access capable persons to handle even complex anonymous payment schemes [15].

Once the hostage-taking has been executed (or faked), the ransomware becomes visible to the victim, for instance with an exemplary message on the dashboard monitor as shown in Figure 3. Such an extortion message usually explains the actual blackmail situation and provides very detailed help and information on how to pay the demanded ransom.

Figure 3: Exemplary in-vehicle extortion message displayed at the in-vehicle infotainment unit.

3.5 Ransom Payment Procedure

In case the victim is willing to pay the demanded ransom, the ransomware client has to provide a fast, simple, user-friendly, and particularly an anonymous payment channel. In contrast to former approaches for ransom payments like premium SMS, straw man accounts, or even physical currency, todays approaches using cryptographic currencies can ensure the above-mentioned requirements. As shown in Figure 4, this can be done simply out-of-the-box using for instance widely available smartphone apps that easily change and transfer virtually all physical currencies into anonymous cryptographic currencies like Bitcoin. In case the attacker really wants to release the vehicle after a successful ransom payment, the payment procedure has to create and include some unique vehicle identifier in order to associate the corresponding vehicle with the paid ransom. This

notification could be part of the payment scheme (e.g., vehicle individual payment target addresses) or (less reliably) an encrypted individual message from the ransomware client to its bot master.

Figure 4: In-vehicle ad-hoc payment of demanded ransom with a common Bitcoin-capable finance smartphone application.

3.6 Release of the Target Vehicle

Assuming that (i) the victim has accepted and successfully managed to actually pay the demanded ransom, (ii) the attacker was able to associate the paid ransom uniquely to the corresponding vehicle (cf. Section 3.5), (iii) the attacker is willing and able(!) to release the in-vehicle component taken hostage (cf. Section 3.4), and (iv) the attacker has a secure and concealed ad-hoc communication channel to the in-vehicle ransomware client or the ransomware victim (e.g., direct Internet connection to the ransomware client, SMS or email to victim, dedicated webpage etc.) in order to communicate the necessary release parameters (e.g., secret command, password, PIN, recovery or decryption key, UDS commands etc.).

Even though all these assumed capabilities could turn out to be some considerable hurdles technically, in classical IT, up to 70% of the ransomware business victims and ~50% of consumer victims actually pay the ransom. This totalled to roughly $1 billion in 2016 (cf. Section 1 "Ransomware Is Already a Very Successful Security Threat in Business IT"). In fact, in order to keep victims paying the ransom, it is necessary that there is at least some realistic chance to get the hostage released once the ransom has been paid.

Figure 5: Vehicle extortion release message displayed at infotainment unit after demanded ransom has been paid.

4 Proof-of-Concept Vehicle Ransomware Attack

In order to validate the vehicular ransomware attack scheme, we developed a basic proof-of-concept demonstrator to execute a ransomware attack against a real vehicle ECU as shown in Figure 6.

Based on the general vehicular ransomware attack scheme shown and explained with Figure 2, we used:

- A Raspberry Pi with a touch screen running a Linux OS, which poses as the infected host ECU,
- An Arduino microprocessor running bare metal software, which poses as gateway ECU, and
- A real vehicle tachometer ECU running the original firmware, which poses as extortion target ECU.

The host ECU and the target ECU are interconnected via our gateway ECU, which in turn uses a proprietary vehicle bus network. The ransomware malware client is a Python script which "infects" our host ECU via the

USB interface. The ransomware client can then brick the tachometer ECU by (i) overwriting the text in the dashboard display with an arbitrary short textual note ("insert coin") and locks vital functions. As an exemplary functionality, the tachometer has been chosen to show a maximum speed despite the vehicle actually standing still. After the successful lock/brick, the ransomware client overlays the graphical user interface of the infotainment unit with the corresponding extortion message including all necessary information for paying the demanded ransom of 50€ to the respective Bitcoin wallet. Once, the ransom payment has been acknowledged (via key signal), the ransomware client releases the tachometer ECU by enabling it to show the actual vehicle speed again and removing the textual note, before the client finally acknowledges the successful release also at the infotainment unit display before the infotainment unit returns to its original graphical user interface.

Figure 6: Vehicle ransomware proof-of-concept demonstrator setup showing (a, top-left) infotainment unit interlinked with tachometer as the extortion target ECU, connected via a gateway unit, (b, top-middle) an infotainment unit misused as infection entryway into the vehicle via USB interface, to execute the malicious ransomware client, (c, top-right) ransomware client has successfully bricked the tachometer ECU and displays ransom message on the infotainment unit, (d, down-left) vehicular extortion attack target, the tachometer, has been successfully bricked by the in-vehicle ransomware client, (e, down-middle) ransomware client has received "ransom paid" message, and displays a corresponding message on the infotainment unit, and releases the tachometer ECU, (f, down-right) vehicular extortion attack target, the tachometer, has been successfully released by the in-vehicle ransomware client.

5 Protection and Reaction against Vehicular Ransomware

As often with security, there is unfortunately no "one measure that solves all" available. Hence, in Section 5.1 we will provide some recommendations for effective protection measures to reduce the risk for a vehicular ransomware attack. As always with security, there is no 100% protection possible or at least not practicable. Hence, in Section 5.2, we will provide some recommendations for actions in case of a vehicular ransomware attack.

5.1 Recommended Protections to Reduce the Risk of a Vehicular Ransomware Attack

Effective protection and mitigation against vehicle ransomware is – in contrast to classical IT systems – rather difficult and costly, since vehicles so far (i) have more potential attack points, (ii) cannot effectively backup data or functionality, (iii) get no regular security updates, and (iv) have only simple (gateway) firewalls, but no sufficient intrusion detection and response systems.

Hence, the best way to avoid becoming a vehicular ransomware victim is applying a holistic security engineering in advance, which means a complete, systematic, multi-layer protection approach that covers the:

- complete vehicle system (i.e., from individual ECU to connected cloud backend)
- complete vehicle lifecycle (i.e., from first requirements analysis to vehicle phase-out)
- complete vehicle organization (i.e., from security processes to security governance)

The next three paragraphs explain the realization of these three security principles a bit more in detail. However, for full details please refer to [13].

Securing the Complete Vehicle System

To secure the complete vehicle system, we have to consider the whole vehicle system starting from the individual ECU all the way up to the connected services in the backend, since a smart attacker would also check the entire vehicle system for the weakest link at which to most easily execute an attack. For sustainable vehicular security, we also need multiple lines of defense since – especially within the rather slow and costly to adapt vehicular security domain - we always have to assume that one of our protection measures might become weakened or even fail. Long term, real-world security experience forbids the typical "single point of failure" protection approaches which might have, for instance, only a single firewall gateway isolating a secure internal vehicle network from an insecure external one, and where a single vulnerability would compromise all vehicles of that type in the world completely and at once.

When considering the typical attack scheme of a vehicular ransomware attack as described in Section 2, we recommended to realize the following (technical) protection measures shown in Figure 7 and (due to the page limitations) shortly described in the following in order to attempt breaking the attack path as often as possible.

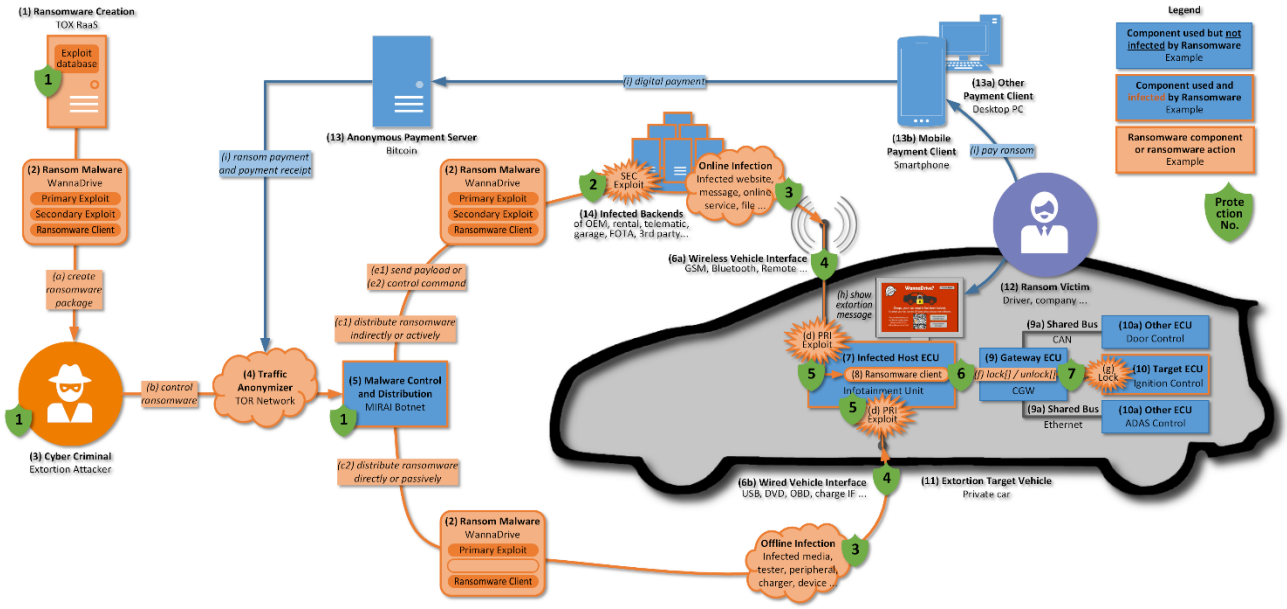

Figure 7: Technical protection measures (green shields) against vehicle ransomware attack scheme.

1. Vehicle Cyber Security Intelligence & Research

Attackers will look for deficiencies in all components including hardware, firmware, driver, operating system, software, libraries and more. From an intelligence perspective, companies should prepare accordingly and check all of their components for published flaws continuously. When using a botnet to distribute the ransomware, overlay network architectures should be able to identify this (e.g., via IDS). Vehicle cyber security intelligence should further support relevant cyber security research, attend relevant security events, monitor relevant websites and organizations, and make relevant strategic cooperation to detect and prepare against a potential ransomware attack as soon as possible.

2. Classical Enterprise Security for all Vehicle IT Infrastructures

When realizing enterprise-level IT-security concepts, following best practices will greatly help to prevent ransomware infections and their spread via infected vehicle IT infrastructures. This includes but is not limited to taking care of patching, access control, network security (firewall, IDPS, MILS, DMZ, segregation, general monitoring etc.), endpoint protection, email protection, data protection (e.g. encryption, media control) and backup, general business continuity management, and disaster recovery. Please refer to classical network security literature for further details.

3. Strong Backend Access Control for all Vehicle-related Assets, Interfaces, and Functionalities

Additional to classical network security, it is essential to limit the external access to vehicle assets, interfaces, and function to a minimum, which means only for the minimum number of authorized persons or devices actually needed, only for their authorized task, and only for the time needed. All other access rights should by denied by default. Authorized entities should authenticate themselves only with strong cryptographic

authentication mechanism such as two-factor authentications support for instance with smartcards. In order to ensure strong access control to the complete vehicle wired and wireless interfaces, necessary access rights, security credentials etc. should centrally managed by a dedicated vehicle security expert organization (cf. following paragraph about securing vehicle organizations).

4. Complete Vehicle Interfaces Protection

All non-essential vehicle interfaces (e.g., debug interfaces) should be removed completely. All remaining wired and wireless interfaces should accessible only with strong cryptographic authentication, limit their accessible functionality and limit their inter-domain communications to the strictly necessary while isolating their functionality behind as strong as possible (e.g., via physical or logical isolation). All vehicle interfaces should further provide some monitoring functionality in order to enable internal and/or external intrusion detection systems to detect (and prevent) any malicious behavior (e.g., brute force attacks) as soon as possible.

5. Secure Vehicle E/E Architecture

Describing the details of how to effectively secure a whole vehicle E/E architecture would go far beyond the scope of this paper, but can be found for instance here [33]. Hence, we will give only some examples for some particular anti-ransomware best practice principles such as:

- Ensure proper vehicle security awareness and apply systematic vehicular security engineering [34],
- Minimizing digital interfaces, access rights and interactions to those absolutely necessary (e.g., whitelists only, deny-by-default), which is a part of "system hardening" or "reduction of attack surface"
- Isolate where possible especially in-vehicle domains with different security and/or safety requirements (e.g., physically isolated ECUs, kernel separation architectures, Trusted Execution Environment (TEE), Smartcards, Trusted Platform Modules (TPM))
- Consider contradictory requirements and necessary actions when facing challenges regarding the concepts "fail secure" vs. "fail safe" vs. "fail operational" (e.g., ECU ROM emergency mode).
- Enable secure(!) over-the-air software updates for all critical in-vehicle software components and all software-based in-vehicle security protection mechanisms.
- Give the driver or trusted in-vehicle actuators the chance to switch some non-essential vehicular components (e.g., telematics) off or in "safe mode" in order to contain a potential ransomware attack.
-

6. Vehicle Intrusion Detection and Prevention System

A vehicle intrusion detection and prevention system (IDPS) will help to defend against ransomware especially by detecting and preventing malicious activity being used to propagate the ransomware infection within the vehicle and between vehicles. Thus, vehicle IDPS monitor all in-vehicle bus systems and external vehicle interfaces for anomalies, report and evaluate anomalies either locally or (better) remotely to a central defense center. There, together with the IDPS reports from million other vehicles and by applying AI-based heuristics, big data analyses, and manual evaluation of dedicated vehicle security expert teams [35] large-scale vehicle ransomware attacks might become prevented or at least become contained.

7. Automotive In-vehicle Firewall

An in-vehicle firewall will check all internal as well as all incoming and outgoing vehicle communication trying to filter out all malicious data and communications based on (regularly updated) attack signatures, white- and blacklists, plausibility checks etc. Please refer to [36] for further details.

8. Incident Response Procedure

In some cases, despite all precautions, a vehicular ransomware attack may succeed and then might evolve. We propose the emergency response procedure as described in Section 5.2 to repel and contain a vehicular ransomware attack.

Securing the Complete Vehicle Life-Cycle

In contrast to classical engineering, where the later operational environment is mainly defined by natural laws and reliability statistics and where engineering processes hence usually end with the start of production, security engineering has to continue until vehicle phase-out. This is because the security environment is continuously changing, particularly in early production, or when newly identified attack paths, new vulnerabilities, or new security research approaches are discovered. Thus, for a holistic vehicle security approach, we have to secure

the complete vehicle life-cycle continuously as shown Figure 8 in including some exemplary security procedures executed during each lifecycle phase.

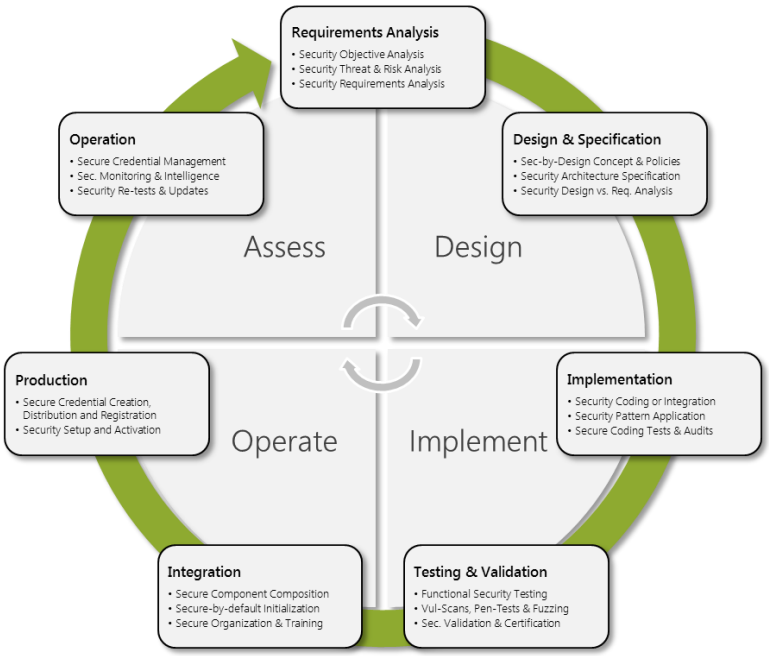

Figure 8: Continuous vehicle security lifecycle with exemplary security operations per lifecycle phase, which are executed continuously until product phase-out, to be able to react to the continuously changing security environment.

Such a continuous lifecycle also has some additional technical and organizational implications, since for instance all development hardware, all tool chains, and at least some of the experts involved have to remain available until final phase-out, which means for heavy-duty vehicles: for up to 20 years.

Securing the Complete Vehicle Organization

Holistic vehicle security is indeed much more than "just another feature" developed by "just another department". In fact, holistic vehicle security requires deep cross-divisional integration and strong commitment from the whole organization including dedicated budget, people, and authority. This is especially difficult since security, at first glance, creates neither new features nor new revenues, but only additional processes, documentation, and complexity, without any immediately apparent benefits.

Without engaging the whole organization, the efforts for security can become quickly ineffective and bogged down by competence disputes, incompatibility, double work, which can cause important security work to be simply omitted due to other (short-term) goals. On the other hand, a well-engaged security organization helps a lot for instance to avoid inefficiency by several mutually incompatible isolated or "silo-ed" solutions (also known as "Insellösungen"). It also clearly reduces security risks by reducing complexity ("which is the worst enemy of security"), provides always a good system overview and ensures proper management of all security-critical functions and corresponding credentials. Moreover, well-organized vehicle security management can in fact increase security without extra costs, for instance, if small separate security mechanisms can together share a powerful high-security hardware crypto module.

A vehicle security organization, which is an independent and additional structure to the classical IT security organization, focusses on the cybersecurity protection of the vehicle (or its components) and introduces new security organizational units, roles, and relationships such as:

- *Vehicle Security Expertise Center* (VSEC) that realizes the vehicle security governance for the company amongst others by developing, maintaining, and auditing relevant vehicle security procedures, guidelines, and policies, and by steering and cooperating amongst others with security intelligence & research teams, legal departments, and company management regarding all vehicle security issues.

- *Vehicle Security Monitoring and Incident Response Team* (VSMIRT) that evaluates (new) security risks and threats, conducts vehicle security forensics, and, if needed, coordinates the development, rollout and communication of all response measures such as security patches.
- *Vehicle Security Officers* (VSO) who are involved in all (technical) organizational units to consult and ensure relevant vehicle security procedures, guidelines, policies, and protection measures from VSEC and who reports new security risks, requirements, or improvements (if any).
- *Chief Vehicle Security Officer* (CVSO) who is heading the VSEC and hence all vehicle security activities and strategies of a company and who reports directly to the management board in order to push necessary security requirements, decisions, and measures through all other company departments.

Since the details of how a vehicle manufacturer or supplier could secure the complete organization would again go beyond the scope of this article, we would have to refer to relevant literature for further details.

5.2 Recommended Actions in Case of a Vehicular Ransomware Attack

Security experts usually recommend not paying the requested ransom since unlocking the digital device/data is often not done even if the ransom has been paid, or since unlocking may not be possible, and especially to avoid promoting imitators [14]. However, in some urgent cases and to avoid further larger damages, paying the ransom might be a valid option, even though there is a considerable risk that it might not work out. Thus, in case of a successful vehicular ransomware attack, we propose the following procedure (nonetheless, even then we assume the following minimal prerequisites in order to do a meaningful response):

- Experienced vehicle security expert team (cf. VSEC in Section 5.2) for centrally monitoring and managing all necessary actions, communications, and decisions.
- Vehicle-specific security emergency response plan for having options, actions, decisions, tools, experts, management etc. properly prepared in order to be able to react quickly and effectively.
- Remote software update functionality in order to quickly and widely roll-out the defined ad-hoc countermeasures (cf. following paragraph) and security patches that have been exploited by the ransomware in order to release already extorted vehicles and protect all other vehicles against this attack.

Based on these prerequisites, we recommend as shown in Figure 9 the following emergency response procedure to repel and contain a vehicular ransomware attack.

1. Detection of vehicular ransomware as early as possible by reports of first victims (worst case) or by the dedicated cyber security intelligence team of the company, which continuously monitors relevant attacker venues (e.g., forums, IRC), security conferences, and potential cyber criminals, but especially evaluates the feedback from vehicular intrusion detection tools that continuously monitor external and internal vehicle networks for suspicious activities using for instance on heuristics, big data analyses, artificial intelligence, and human security expertise.
2. Analyses of vehicular ransomware by vehicle security experts once a (potential) attack has been identified by analyzing possible in-vehicle and infrastructure attack paths, the ransomware client itself, its extortion mechanisms, it remote control for possible security exploits, but also for possible attacker and attack motivations.
3. Security risk evaluation and vulnerability assessment by vehicle security experts based on systematic evaluation [30] for corresponding attack potentials (e.g., coverage, spread rate, complexity) and damage potentials (e.g., vehicle safety, financial, operational, reputation damages).
4. Identification and evaluation of possible ad-hoc countermeasures and responses (including paying the demanded ransom) by vehicle security experts amongst others for their feasibility, effectiveness, potentially creating (other) new risks in order to mitigate the most critical security risk and vulnerabilities that have been evaluated before.
5. Decision by company management based on security expert proposals for response measures (e.g., technical and non-technical measures), incident response communication, further risk provisioning etc.
6. Development, testing, and preparation, coordinated by vehicle security experts of:
    a) Technical response measures such as providing ECU backup firmware/data/credentials, vehicle and/or infrastructure software (security) patches, ECU/vehicle re-configuration commands, targeted deactivation or isolation of affected vehicle functionality, updated access rights, updates firewall rules, updated malware signatures or even active cyber counter-attacks (e.g., Denial-of-service attacks against ransomware control infrastructures).

b) Non-technical response measures such as “attacker diplomacy”, ransom payment, informing general cyber defense authorities (e.g., industry or national institutions) and police, or legal actions (if possible).
c) Incident response communication within the company and towards customers, supplier, partners, industry committees, public authorities, or media.

7. Roll-out of technical, non-technical response measures, and starting incident response communication.
8. Continuous monitoring and (re-)evaluation of impacts, risks, and success from all executed response measures for adaption of measures or further/less measures (e.g., in the case of a step-by-step approach) until ransomware attack is repelled or at least sufficiently contained.
9. Investigation and security forensics for documentation and reporting, but especially for long-term containment, complete recovery, lessons-learned, prevention measures, and updated monitoring.

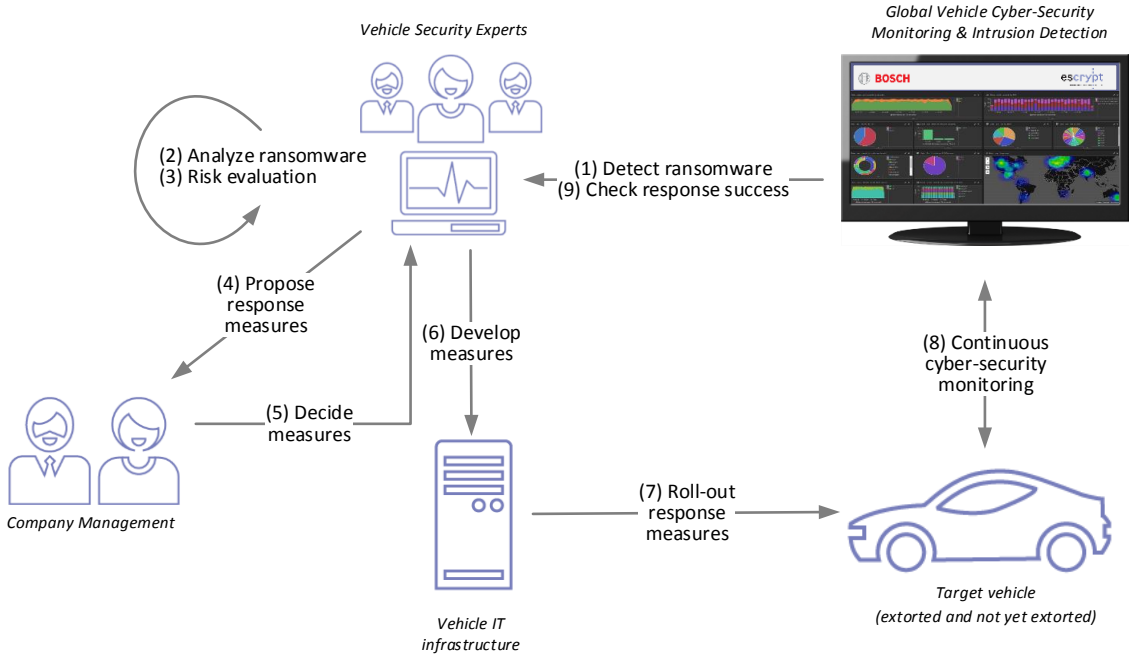

Figure 9: Recommended emergency response procedure in case of a vehicular ransomware attack

6 Summary

Ransomware on vehicles has the potential to become a real threat to vehicles for the same reason that it has become a significant and persistent menace to IT infrastructure in institutions and businesses: there is a compelling business model. Victims of ransomware on vehicles will also have compelling reasons to pay the ransom demanded to regain access to their vehicles, or to restore their vehicles to a properly functioning state. Looking at the “marketplace” for vehicle ransomware, we have argued that commercial vehicles and large vehicle fleets are probably the most tempting first attack targets for ransomware.

We have also shown that vehicle ransomware can be readily created and deployed, showing that that threat of ransomware on vehicles is real and present. We have also argued that, as vehicles become more and more interconnected, and as digital technology continues to provide more and more essential vehicle features (such as advanced driver assist), and paradoxically, as vehicle digital technology becomes more standardized, that the attack surfaces for ransomware will increase, the value that ransomware can take hostage will grow, and the population that a single strain of ransomware can target will expand.

We have also argued that, in concert with the growth and importance of interconnected information technology in vehicles, that the industry must also prepare for ransomware attacks by extending to vehicles protection capabilities at the same rapid rate, preparing ahead for the threat with holistic multilayered protections, but also extending to vehicles the ability to react to attacks with updated defenses and responses.

7 References

[1] Stephen Checkoway et al., “Comprehensive Experimental Analyses of Automotive Attack Surfaces”, USENIX Security Symposium, 2011.

[2] Karl Koscher et al., “Experimental Security Analysis of a Modern Automobile”, IEEE Symposium on Security & Privacy, 2010.

[3] Andy Greenberg, “Hackers Reveal Nasty New Car Attacks – With Me behind the Wheel”, forbes.com, July 2013.

[4] Keen Security Lab, “Car Hacking Research: Remote Attack Tesla Motors”, keenlab.tencent.com, September 2016.

[5] Jay Turlay, Mazda Infotainment USB Port PoC Attack, https://github.com/shipcod3/mazda_getInfo

[6] Iain Thomson, “Stop the music! Booby-trapped song carjacked vehicles – security prof”, The Register, January 2016.

[7] Ian Foster, “Fast and Vulnerable: A Story of Telematic Failures”, USENIX Workshop on Offensive Technologies (WOOT), 2015.

[8] Troy Hunt, “Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs”, troyhunt.com, February 2016.

[9] Financial Times, “Honda plant hit by WannaCry ransomware attack”, ft.com, June 2017.

[10] The Telegraph, “Cyber-attack hits German train stations as hackers target Deutsche Bahn “, May 2016.

[11] CNET, “South Korean web host pays largest ransomware demand ever “, cnet.com, June 2017.

[12] Malwarebytes Inc., “Understanding the Depth of the Global Ransomware Problem”, August 2016.

[13] Thomas Wollinger, “A Holistic Security Approach for Automotive”, Automobil-Elektronik-Kongress Ludwigsburg, June 2016.

[14] No More Ransom Initiative, www.nomoreransom.org, 2017.

[15] IBM X-Force Research. “Ransomware: How Consumers and Businesses Value Their Data”, 2016.

[16] Malwarebytes Inc., “Cybercrime Tactics and Technologies”, July 2017.

[17] Herstellerinitiative Software (HIS), SHE Secure Hardware Extension Version 1.1, 2009.

[18] Stephanie Bayer et al. “Security Crash Test – Practical Security Evaluations of Automotive Onboard IT Components”, Automotive Safety & Security, 2014.

[19] McAfee Labs, “Meet ‘Tox’: Ransomware for the Rest of Us”, May 2015.

[20] Symantec Blog, “Mirai: what you need to know about the botnet behind recent major DDoS attacks”, October 2016.

[21] Catalin Cimpanu, “You Can Now Rent a Mirai Botnet of 400,000 Bots”, bleepingcomputer.com, November 2016.

[22] Craig Smith, “Car Hacker's Handbook”, opengarages.org/handbook/, 2016.

[23] Jan Schüßler, “Erpressungstrojaner "Highwayman" zielt auf Autofahrer“, heise Security, April 2017.

[24] Digital Guardian, „History of Data Breaches“, https://digitalguardian.com/blog/history-data-breaches

[25] Bleeping Computer, “About 90% of Smart TVs Vulnerable to Remote Hacking via Rogue TV Signals”, https://www.bleepingcomputer.com/news/security/about-90-percent-of-smart-tvs-vulnerable-to-remote-hacking-via-rogue-tv-signals/

[26] Techcrunch, “Project Zero uncovers a nasty Wi-Fi chip exploit”, visited 17.07.2017, https://techcrunch.com/2017/04/04/project-zero-uncovers-a-nasty-wi-fi-chip-exploit/

[27] Google Project Zero, “Over The Air: Exploiting Broadcom’s Wi-Fi Stack (Part 1)”, https://googleprojectzero.blogspot.de/2017/04/over-air-exploiting-broadcoms-wi-fi_4.html

[28] Google Project Zero, “Over The Air: Exploiting Broadcom’s Wi-Fi Stack (Part 1)”, https://googleprojectzero.blogspot.de/2017/04/over-air-exploiting-broadcoms-wi-fi_11.html

[29] Google Project Zero, visited on 17.07.2017, https://googleprojectzero.blogspot.de/

[30] Michael Scheibel et al., “A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems", In Automotive Safety & Security, November 2012.

[31] Atinderpal Singh, “A look at recent STAMPADO ransomware variant”, Zscaler Blog, November 2016

[32] The TOR Anonymity Network Project, www.torproject.org, July 2017.

[33] Marko Wolf, “Security Engineering for Vehicular IT Systems”, Springer+Vieweg-Verlag, 2009.

[34] SAE J3061, “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems”, Work in progress, 2017.

[35] Jan Holle, “Automotive Intrusion Detection and Prevention System (IDPS)”, ConCarForum, 2017.

[36] Karsten Schmidt et al., “Hardware and Software Constraints for Automotive Firewall Systems”, SAE Technical Paper 2016-01-0063