MISSIONE 4
ISTRUZIONE
RICERCA

FORESEEN

Deliverable D1.2 - Report on threat analysis and identification of critical physical devices

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
Università di Pisa

MISSIONE 4
ISTRUZIONE
RICERCA

FORESEEN

FORmal m**E**thod**S** for attack d**E**t**E**ction in autonomous drivi**N**g systems

PRIN 2022 PNRR

Project number: P2022WYAEW
CUP: I53D23006130001

Deliverable D1.2: **Report on threats analysis and identification of critical physical devices**

Project Start Date: 30/11/2023 **Duration**: 24 months

Coordinator: *University of Pisa*

Deliverable No	D1.2
WP No:	WP1
WP Leader:	RU-PA
Tasks:	T1.3 - Leader: RU-MI
Due date:	M3-6
Delivery date:	May 31, 2024
Authors:	RU-MI, RU-PA, RU-PI

Dissemination Level:

PU	Public	X
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

Contents

List of Acronyms

CACC	Cooperative Adaptive Cruise Control
CAN	Controller Area Network
CPA	Correlation Power Analysis
CPS	Cyber Physical System
DoS	Denial of Service
ECU	Electronic Control Unit
OBD	On Board Diagnostic
V2E	Vehicle to Edge
V2N	Vehicle to Network
V2V	Vehicle to Vehicle

1. Introduction

The content of this deliverable shows the results of a preliminary phase for the threat analysis of the platooning system. Here we will analyze the possible access points for an attacker over the system, starting by studying the state of the art for attacks on vehicles and vehicular networks.

The final result of this task will be the identification of the access points and critical devices on the platoon modeled in Deliverable D1.1.

2. Attack surfaces on modern vehicles

Modern vehicles are highly computerized, making them potentially vulnerable to attacks. Interesting studies have been made regarding this topic. In the following, a brief explanation of which could be the access points used by attackers and the consequences of the exploitation of the latter will be given. In particular, in [Checkoway 2011], a comprehensive analysis of automotive attack surfaces is reported. It is shown that there are many ways in which an attacker could get full control over a computerized car, since he could obtain access indirectly via various ports. The attack types that are considered are indirect types of attacks and they have been developed and tested on a vehicle, proving that the considered vulnerabilities could actually be exploited by a potential attacker. The following attacks were tested:

- *OBD-II*: On-board diagnostics Parameter IDs are codes used to request data from a vehicle, used as a diagnostic tool. Those are commonly used by service personnel during routine maintenance. On modern vehicles a PC-centric approach is used, meaning that the Software on a PC is the software that gets connected to the car in order to retrieve and send data. If one is able to compromise the computer used for diagnostic, he can also get full control over the vehicle.
- *Media Player*: After studying the firmware of a media player of a vehicle they were able to create a CD containing malicious data which will be elaborated by the car.
- *Bluetooth:* Via reverse engineering, they managed to obtain information about the Unix-like Telematics ECU’s operative system. After analyzing that, they found many wrong usages for the function strcpy, which could be easily exploited.

Moreover, modern vehicles also have cellular capabilities, thus leading to a wider range of vulnerabilities (*Cellular network*).

All the attacks presented in the paper provided the malicious user full access to the car, thus allowing the hacker to do whatever he wants. The threats associated with each of those attacks are many, for example *theft* and *surveillance* are a possibility.

Theft would be quite easy since the only thing that needs to be done is to make the car unlock itself, but a more expert attacker could do much more. By compromising a large number of vehicles using any of the listed possible exploits, the attacker could, by using the car’s GPS and cellular line, report back to a central server information about the vehicle, in order to have a set of compromised car, their specification and position. The latter is only a hypothetical scenario, but the authors of the paper were able to implement an attack that unlocked the car, started the engine and blocked any anti-theft mechanisms, allowing anyone to steal the vehicle with no effort simply by driving it away.

Surveillance is also possible once a hacker has full control over the car, in fact, it has full access to its GPS, making him know its position, but could also allow him to activate the in-cabin microphone and collect audio recordings of the drivers, possibly eavesdropping private or sensible conversations.

The two examples provided above are not the whole set of possible threats, in fact throughout the attacks listed before it is also possible to access the engine and brakes, making the vehicle completely unsafe since an attacker could remotely force it to accelerate, disable brakes or abruptly stop. Attacks that modify the data provided from the sensors to the Controller, comprise the *safety* of the system.

Moreover, with modern *cryptographic algorithms*, the communication is often considered to be safe from external attacks. This is because brute-forcing a key is generally really hard, and, in most cases, it is impossible to leak any useful information regarding the plaintext or the key itself.

For what concerns the V2V communication, the IEEE 1609.2 standard is taken into account. This standard uses the AES-CCM cryptographic algorithm for the symmetric encryption of data during the run. While this algorithm is very powerful against brute-force and guessing attacks, especially if the key is properly generated at the beginning of the communication session, it is known to be vulnerable to a side channel attack called *Correlation Power Analysis* (CPA).

Moreover, assuming that a potential attacker got access to the Controller of the vehicle in one of the possible ways listed above, it would be fairly possible for him to alter the symmetric key generation phase at the beginning of the communication session, thus obtaining the key.

3. Threat analysis and identification of critical devices

In this section, we will focus on threats and critical devices related to platoon application, by considering vulnerabilities and threats that may compromise the platoon safety, string stability and fuel saving benefits. For a complete overview of threats and attacks to connected autonomous vehicles refer to [El-Rewini 2020, Filho 2024], which provide a board analysis of many aspects and challenges about threats, attacks to connected and cooperative vehicles.

Considering the communication networks within the vehicle, the CAN (controller area network) bus represents one of the most critical communication bus, because it is responsible of transport data from/to the powertrain and on-board sensors. Altering the data or delaying them could cause serious consequences for safety and significantly compromise the performance of the platoon. In the following we analyse the different attacks to CAN bus that represent concrete threats for platooning:

- *Injection attack*: attackers insert fraudulent messages into an automotive bus system using OBD-II ports, compromised ECUs, or infotainment and telematics systems as access points. Because the traditional CAN protocol does not authenticate the nodes that send or receive messages, it cannot detect illegitimate frames. Injecting fake messages regarding data and instructions could alter the behaviour of entire platoon, because these fake data are also sent to other vehicles (V2V communication approach) or to remote platoon controller (V2N communication approach); thus, altering the representation of the platoon in the cyber space. Similarly, fake instruction messages issues wrong signal to powertrain modules that do not reflect the desired acceleration instruction provided by the control law computation (e.g., CACC). Without tailored countermeasures, other vehicles, as well as the compromised vehicle are unable to distinguish between real and fake messages as CAN bus does not provide specific integrity and identification features.

- *Replay and Denial of Service (DoS)*: attackers repeatedly resend valid frames or high-priority messages to disrupt the vehicle's real-time operations obstructing legitimate and low-priority messages to be sent on the bus. This attack causes delay in collecting data from on-board sensors or implementing the acceleration instruction. These two attacks could significantly alter the behaviour of the compromised vehicle and, as consequence, the entire platoon as other vehicles and remote controller rely on timing messages to maintain a coherent cyber representation of the platoon.

Considering the V2V and V2N communication network, we focus on attacks that cause communication delays and alteration of the cooperative perception, e.g., illusion, sybil, impersonation, and alteration/replay attacks. Differently from the attacks that exploit the intra-vehicle communication network, attacks performed using inter-vehicle communication network can be performed also by vehicles that are not part of the platoon. For this reason, attacks through V2V and V2N communication network represent significant threats for platoon CPS. It is worth mentioning that we assume that the attackers are able to break privacy and integrity of the platoon application, both on board and on the edge, preventing the platoon vehicle to distinguish between legitimate and forged messages.

In the following, we present the major threats resulting for running attacks from compromised vehicles (within and external to the platoon) exploiting V2V and V2N communication.

- *Illusion attack*: in an illusion attack, attackers manipulate vehicle sensor readings to send false traffic information from legitimate sources. This causes other vehicles to make incorrect decisions. Detection is difficult because messages are considered legitimated by the vehicles. Of course, this attack is safety-critical, because it can induce unexpected and unpredictable behaviour of the platoon, e.g., sudden breaking as a reaction of fake emergency breaking or obstacle information.
- *Sybil attack:* in this case a single intruder vehicle can declare itself as multiple vehicles, leading to extensive alteration of communication topology and consuming large amounts radio resources. From the platoon point of view, this attack can cause a wrong perception of the traffic situation surrounding the platoon, leading to unexpected and unpredictable reaction. Moreover, this attack could also alter the actual composition of the platoon, because the phantom cars can be perceived as part of the platoon. As for the illusion attack, the sybil attack significantly alter the cyber representation of the platoon leading to serious consequences for the safety, disrupting the platoon.
- *Timing attack:* in a timing attack, a malicious vehicle receives a message, delays it, and then forwards it to other vehicles, causing incorrect timing information. Being the platoon system highly sensitive to delayed messages, this attack alters the cyber representation of the platoon, causing imprecise instruction computation.
- *Jamming and DoS (DSRC & Cellular)*: these types of attacks disrupt the communications causing delays and altering the cyber representation of the platoon. Similarly to the attacks presented before, these attacks lead to safety-critical conditions, significantly altering the platoon coordination.

4. Roadmap for future work

This deliverable reports on critical devices and possible access points that can be exploited for cybersecurity attacks in CAV systems, where vehicles are highly computerized thus introducing more space for vulnerabilities. The next step will be the identification of attack scenarios, that will be applied to the platooning use case.

5. Bibliography

[Checkoway 2011] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. “Comprehensive Experimental Analyses of Automotive Attack Surfaces”. In: 20th USENIX Security 98 Symposium (USENIX Security 11). San Francisco, CA: USENIX Association, Aug. 2011.

[El-Rewini 2020] Zeinab El-Rewini, Karthikeyan Sadatsharan, Daisy Flora Selvaraj, Siby Jose Plathottam, Prakash Ranganathan, “Cybersecurity challenges in vehicular communications”, Vehicular Communications, Volume 23, 2020, 100214, ISSN 2214-2096

[Filho 2024] Vasconcelos Filho, Ê., Severino, R., Salgueiro dos Santos, P. M., Koubaa, A., & Tovar, E. (2024). “Cooperative vehicular platooning: a multi-dimensional survey towards enhanced safety, security and validation”. Cyber-Physical Systems, 10(2), 123–175.

[Lo 2016] Lo, O., Buchanan, W. J., & Carson, D. (2016). Power analysis attacks on the AES-128 Sbox using differential power analysis (DPA) and correlation power analysis (CPA). Journal of Cyber Security Technology, 1(2), 88–107.