University of Pisa
School of Engineering

Formal Methods for Secure Systems

An ADVISE model for attacks on autonomous vehicles back-end servers

Supervisors
Prof. Cinzia Bernardeschi
Ing. Maurizio Palmieri

Students
Yuri Mazzuoli
Francesco Iemma
Marco Pinna

July 12, 2021

Contents

1 Introduction **2**

2 Overview **3**
2.1 Actors 3
2.2 Attacker's Profile 4
2.3 Goals 5

3 Attack tree **6**
3.1 Attacks 8

4 Simulation **10**

Chapter 1

Introduction

In what follows the study of different adversaries trying to attack the back-end servers related to autonomous vehicles is carried out.

The work is organized as follows:

- Firstly, chapter 2 gives an initial overview and a presentation of the scenarios.
- Secondly, in chapter 3 the complete attack tree is presented.
- In chapter 4 the development of the Mobius simulation is described and its results are presented.

The entire codebase is available at `https://github.com/YuriMzz/vehiclesADVISE` .

Chapter 2

Overview

In this chapter a general overview of the scenarios and the involved actors is given.
The final goal for each one of the attackers it to gain access to the back-end servers related to self-driving vehicles. This goal can be reached by means of different knowledges, skills and types of attacks, which all differ from one adversary to the other.

2.1 Actors

Three different types of actor have been identified:

Insider

An insider is defined as someone who belongs to the company or works for it. They already have, therefore, access to some facilities (depending on their role in the company) and the equipment they contain (PCs, laptops, routers, etc.), the knowledge necessary to perform some tasks (internal network passwords, website and/or database credentials, VPN access, etc.) and possibly the trust of the rest of the staff.
They might also be aware of potential flaws in the company's systems (vulnerabilities in information system, defective equipment, weaknesses of some employees, etc.).
On the other hand, an insider does not necessarily have the skills needed to perform some of the intermediate attack steps needed to reach the final goal.

Physical intruder

A physical intruder is different from an insider since they have less knowledge about the internals of the company. However, they have advanced *physical* penetration testing skills and tools, as well as the knowledge about the company facilities location, security systems and possibly the timetables of employees and/or security personnel.
Therefore they might have access to a bigger number of facilities and spaces (e.g. they might have – or be able to gain – direct access to a server room).

Hacker

A hacker is an external actor with no prior knowledge of the company's systems and no access to its facilities. On the other hand, they have advanced security and penetration skills, in-depth knowledge of the most important and widespread technologies and attacks, as well as the tools needed to perform these attacks on the target systems.

Actor	Skills	Knowledges	Accesses
Insider	Basic/medium IT skills, social engineering	Login credentials (website, LAN, VPN, DB), employees info, vulnerabilities in company's security system	LAN, VPN, DB, facilities, PCs, workstations, routers, switches
Physical intruder	Lockpicking, ???	Facilities location, personnel timetables	Company's external premises
Hacker	Reverse engineering, social engineering, advanced attack and penetration testing	-	Vehicle (i.e. firmware)

Table 2.1: Attackers' skills, knowledges and accesses

2.2 Attacker's Profile

As we have seen each actor has its own set of knowledges, accesses and skills in table **??** it is possible to see the arrangement of them among the attackers.
For what concern the attention of the actors about the probability of detection, the cost of the attacks and the expected payoff, the weights for each of these factors are shown in the table 2.2.

Attacker Name	Cost Weight	Detection Weight	Payoff Weight
Hacker	0	0.1	0.9
Physical Intruder	0.2	0.5	0.3
Insider	0.1	0.5	0.4

Table 2.2: Weights of Attacker Profile

Thus we can see that the choices that attackers done are guided by different things, for instance an insider will prefer to avoid an attack with an high probability of detection, as well as a physical intruder, instead an hacker has not this preoccupation and he will choice the attack with the higher payoff.

2.3 Goals

Attack a vehicle or extract data

The back-end servers can be used as a means to attack a vehicle and/or extract data from it e.g. its position, the destination the driver is heading to etc.

Data breach

Servers can be also attacked to extract sensitive data related to customers

Back-end server service disruption (DoS)

An attacker could also target the back-end server just to take them down and disrupt their service (Denial of Service), causing issues to all the vehicles whose proper functioning relies on it.

Chapter 3

Attack tree

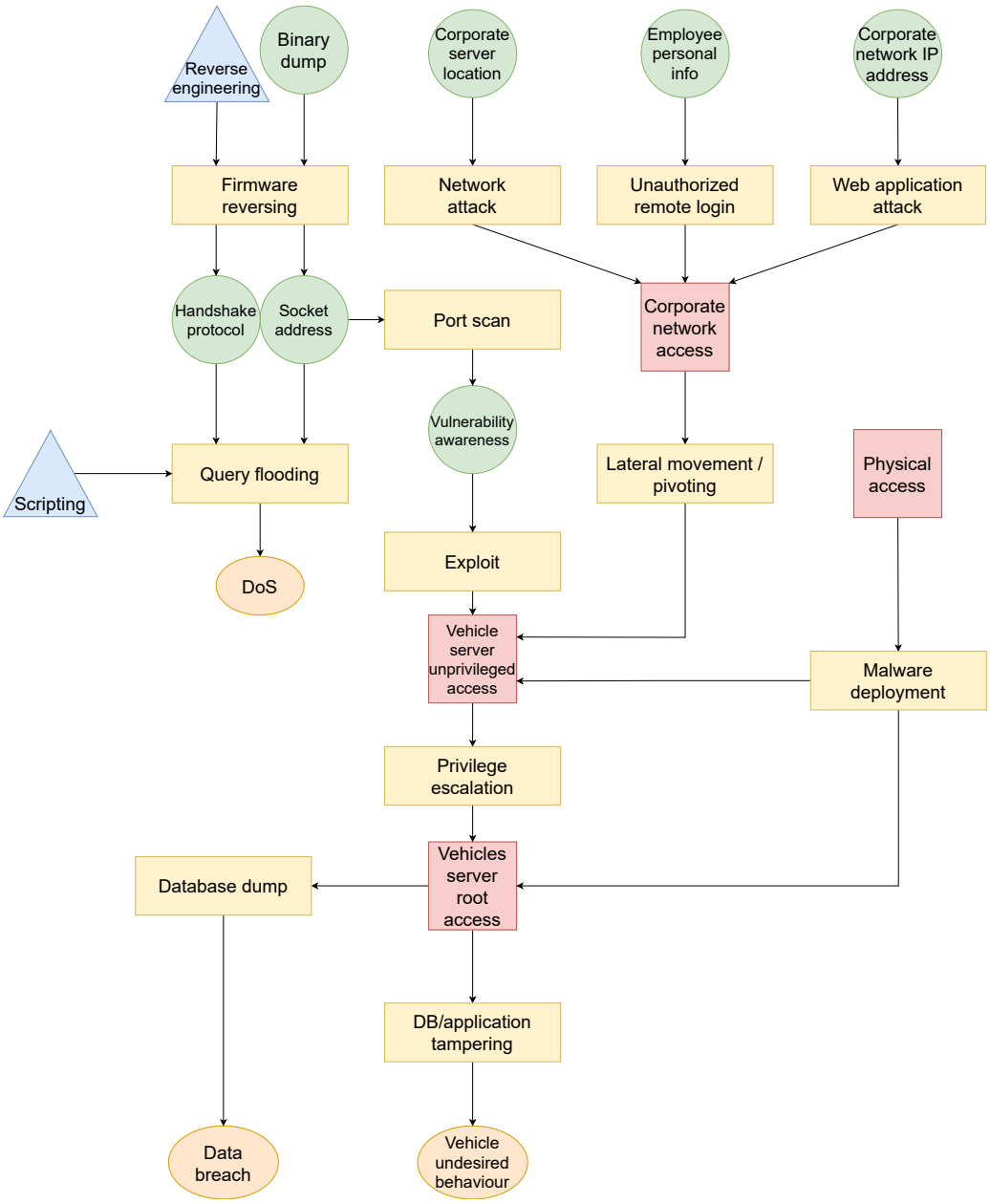

Figure 3.1: Attack tree

3.1 Attacks

Below is a brief description of every attack in the tree:

- **Firmware reversing**: a hacker in possession of a vehicle and with reverse engineering skills can dump the vehicle firmware, reverse engineer it and acquire information about the IP/port of the server, as well as the protocol used for the communication and/or the structure of the messages sent.
- **Query flooding**: a hacker can perform a (D)Dos attack by sending a large number of queries on the server (possibly by means of a botnet) and overwhelming it so that it stops being responsive.
- **Port scan** with the knowledge of the server's IP, a hacker can scan the server for open ports and possibly find out the OS, which services are running and their versions.
- **Network attack** An insider supposedly already has access to the corporate network but, in case they don't, they can either discover the password in a variety of ways (dictionary attack, password re-use, unattended workstations or laptops) or exploit some vulnerabilities in the Wi-Fi protocol.
- **Unauthorized remote login**: an attacker could access the corporate VPN by either discovering some employee's login credentials (e.g. phishing, typosquatting, OSINT, social engineering), exploiting some vulnerabilities in the login procedure itself or by directly having access to credentials (i.e. password dumps found or bought online).
- **Web application attack**: an attacker could gain unauthorized access to a reserved area of the company's website by means of some web-application attacks (SQLi, XSS, XXE, etc.) or backdoors.
- **Lateral movement/pivoting**: an attacker who has already gained access to a part of the network which is not directly the vehicle server, can exploit further vulnerabilities and "move laterally" i.e. move deeper inside the network to find more vulnerabilities and entry points that could lead them to the final target server.
- **Malware deployment**: an attacker can deploy a malware in different ways e.g. dropping an infected USB drive and wait for some employee to plug it in a corporate machine. The malware can guarantee them the access to a server with a varying level of privilege.
- **Privilege escalation**: once an attacker has gained the so-called "foothold" into the target server, they will try to increase their privilege level on the system as to access to a greater number of resources.

- **Database dump**: once the attacker has gained access to the database, the latter can be dumped and the *Data Breach* goal is reached. For the sake of simplicity the `database dump` attack in the tree is considered to have constant time duration and probability of detection. In reality this is not the case as there are different ways to perform data exfiltration, which can be more or less stealthy (simple `scp` or `wget` commands – or their equivalent on non-Unix systems – will be faster but they will also have a high probability of detection while looking at the network traffic and the server logs, while other techniques such as ICMP exfiltration will be stealthier at the expense of a longer time required).
- **DB/application tampering**: if the goal of the attacker is not to access sensitive data but to cause undesired behaviour of the vehicles, once they have access to the DB or the application they can tamper the data in the DB, or attack the application/framework that is running on the server and which interacts with the vehicles.

Chapter 4

Simulation