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

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.

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 arrangment of them among the attackers.

Actor	**Skills**	**Knowledges**	**Accesses**
Insider	basic/medium IT skills, social engineering	login credentials (website, LAN, VPN, DB), employees info, vulns in company security	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)

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 2.1.

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 2.1: 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

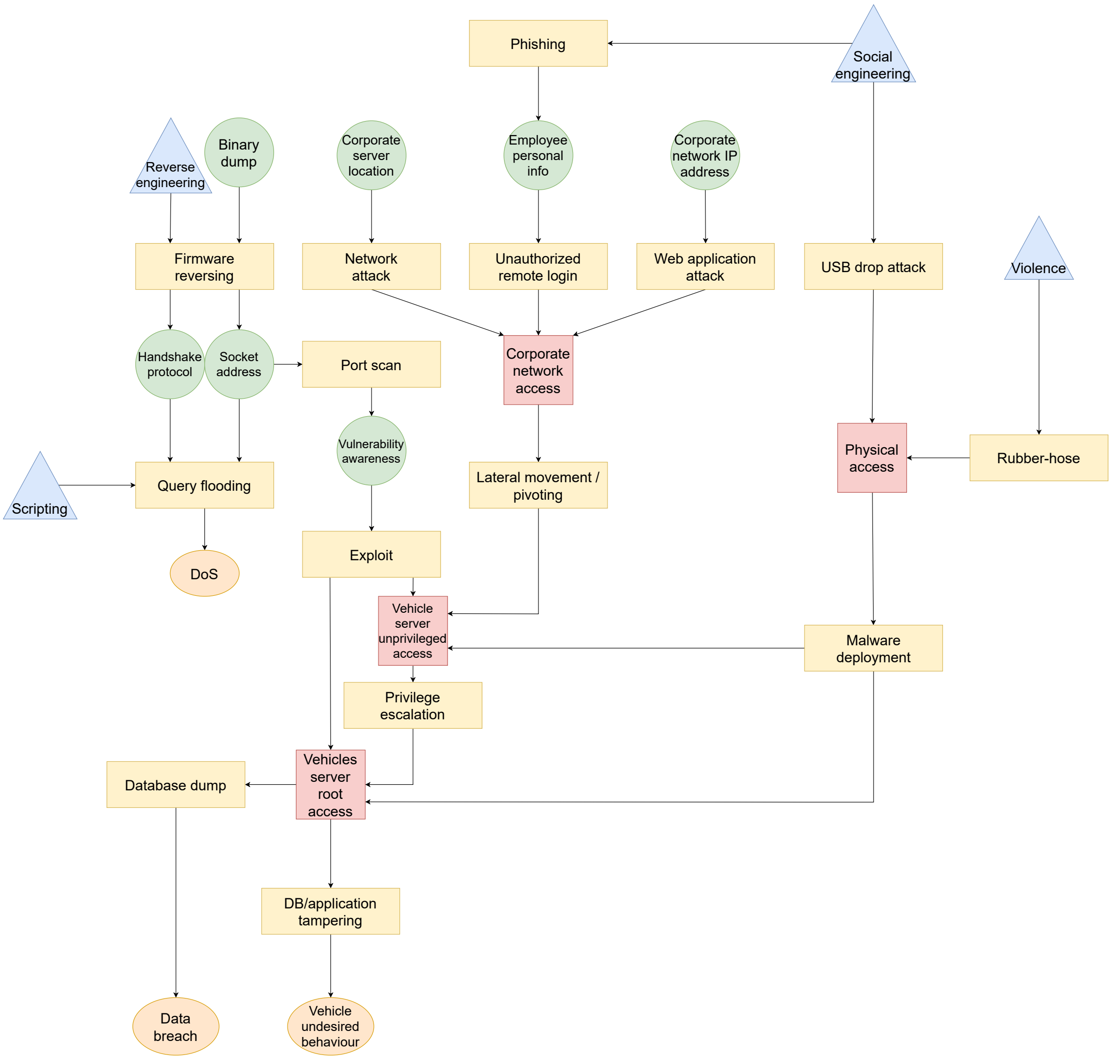

Figure 3.1: Attack tree

Chapter 4

Simulation