

# Report for the CPS Mid-Course Project

Andrea Auletta

`andrea.auletta@studenti.unipd.it`

Niccolò Zenaro

`niccolo.zenaro@studenti.unipd.it`

December 22, 2024

# Contents

<b>1</b>	<b>Introduction and objectives</b>	<b>3</b>
<b>2</b>	<b>System setup</b>	<b>3</b>
<b>3</b>	<b>Experiments</b>	<b>3</b>
3.1	Fabbrication attack . . . . .	3
3.2	Suspension attack . . . . .	3
3.3	Masquerade attack . . . . .	3
3.4	CIDS algorithm . . . . .	3
<b>4</b>	<b>Results and Discussion</b>	<b>3</b>

# 1 Introduction and objectives

In this report we will describe the work done for the mid-course project of the course Cyber-Physical Systems and IoT security. The paper to which we refer is [1] “**Fingerprinting Electronic Control Units for Vehicle Intrusion Detection**” where is explained the design of an algorithm: the CIDS (Clock-based Intrusion Detection System), that is able to detect different kinds of attack. In this paper is shown the functioning of three kinds of attack: the “Fabbriation attack”, the “Suspension attack” and the “Masquerade attack”. What we tried to do was to implement the three attacks and the CIDS algorithm in a simulation environment using **ICSim**, instead of physically as shown in the paper.

## 2 System setup

We worked on a virtual machine with **LinuxMint22** as operating system. The simulator used is **ICSim**. All the code is written in **Python** and can be found at the following link: . We used the **can library** to create messages and to simulate the communication of the attackers with the ECUs.

## 3 Experiments

### 3.1 Fabbriation attack

### 3.2 Suspension attack

### 3.3 Masquerade attack

### 3.4 CIDS algorithm

## 4 Results and Discussion

## References

- [1] Kyong-Tak Cho and Kang G. Shin. “Fingerprinting Electronic Control Units for Vehicle Intrusion Detection”. In: *Proceedings of the 25th USENIX Conference on Security Symposium* (2016), pp. 911–927.