

Projet d’approfondissement / 2021-2022

Filière Informatique - Cybersecurity

**Secure Vehicule To Infrastructure Communication**

Cahier des charges

15.03.2022 – Version 1.0

Denis Rosset

|  |  |
| --- | --- |
| Superviseur :  Mandants : | **Michael Mäder**  **ROSAS**  **Jonathan Péclat**  **Lucio Turaisch** |
|  | Logo  Description automatically generated with medium confidence |

**Table des versions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date de publication** | **Auteur** | **Description** |
| 0.1 | 06.03.2022 | Denis Rosset | Première ébauche du cahier des charges |
| 0.2 | 08.03.2022 | Denis Rosset | Ajout du chapitre des dates clés et des différents jalons du projet dans le planning |
| 0.3 | 09.03.2022 | Denis Rosset | Correction des dates dans la table des versions et modification du planning pour avancer le pentesting et la mise en place du système |
| 1.0 | 15.03.2022 | Denis Rosset | Ajout du schéma global |

Table des matières

[1 Introduction 3](#_Toc98249598)

[2 Acteurs 3](#_Toc98249599)

[3 Contexte du projet 3](#_Toc98249600)

[3.1 But du projet 3](#_Toc98249601)

[4 Objectifs 4](#_Toc98249602)

[4.1 Analyse des communications ITS V2I (WP2) 4](#_Toc98249603)

[4.2 Mise en place de l’OBU et du RSU (WP 3) 4](#_Toc98249604)

[4.3 Spécification de scénarios d’attaques et identification des méthodes et outils offensifs (WP 4) 4](#_Toc98249605)

[4.4 Test d’intrusion (WP 5) 4](#_Toc98249606)

[5 Tâches 4](#_Toc98249607)

[5.1 Analyse des communications ITS V2I (WP 2) 4](#_Toc98249608)

[5.2 Mise en place de l’OBU et du RSU (WP 3) 4](#_Toc98249609)

[5.3 Spécification de scénarios d’attaques et identification des méthodes et outils offensifs (WP 4) 4](#_Toc98249610)

[5.4 Test d’intrusion (WP 5) 5](#_Toc98249611)

[6 Dates Clés 5](#_Toc98249612)

[7 Planning 6](#_Toc98249613)

# Introduction

Ce projet s’inscrit dans le cadre du développement de véhicules autonomes de l’institut ROSAS[[1]](#footnote-2). Le centre de compétences ROSAS (avec l'aide du groupe interdisciplinaire SwissMoves) développe depuis 2018 des technologies permettant d'automatiser les véhicules ainsi que de les conduire à distance via un centre de téléopération[[2]](#footnote-3).

# Acteurs

Ce projet est suivi par les personnes suivantes :

* Denis Rosset, Étudiant en Informatique, MSE
* Michael Mäder, Professeur en filière Informatique et Télécommunication, Superviseur
* Jonathan Péclat, Ingénieur Logiciel, Employé de ROSAS
* Lucio Truaisch, Ingénieur Logiciel, Employé de ROSAS

# Contexte du projet

Un projet HES-SO a été obtenu par l'institut iSIS et ROSAS afin de définir les exigences permettant aux véhicules de communiquer avec l'infrastructure (V2I - Vehicle-to-Infrastructure) de manière sûre et sécurisé. Cette communication permet au véhicule ou au téléopérateur d'être pro-actif est d'identifier les dangers ou obstacles avant de les voir.

## But du projet

Le premier but du projet consiste à mettre en place la communication V2I, respectivement I2V, entre un feu de circulation et un véhicule. Les informations sont échangées à l'aide du standard de communication 802.11p, en utilisant les éléments HW RSU (Road Side Unit - côté infrastructure) et OBU (On-Board Unit - côté véhicule). Puis, l'état du feu de circulation doit être transmis via ITS au centre de téléopération (TCC - Teleoperation Control Center).

Diagram

Description automatically generated

Figure 1 Schéma global du système

Ce scénario de test (Figure 1) sera mis en place sur le site de Bluefactory où se trouve le matériel de communication, le véhicule démonstrateur ainsi que le centre de téléopération. Le second but du projet consiste à tester la sécurité des communications V2I sur la base d'exigences fournies par ROSAS en effectuant du Pentesting (spoofing, replay attack, récupération des informations, Man-In-The-Middle, DoS, etc…). Une section recommandation sera rédigée afin de fournir des propositions d'amélioration pour la sécurité des communications.

# Objectifs

Les objectifs du projet d’approfondissement sont divisés dans différents workpackage utilisés dans ROSAS :

## Analyse des communications ITS V2I (WP2)

Pour effectuer les communications entre OBU et RSU, Le protocole ITS (Intelligent System Transport) est utilisé. Ce protocole est basé sur le Wi-Fi. Afin de pouvoir effectuer les attaques de manière efficace il est nécessaire de connaitre les fonctionnements des protocoles utilisés.

## Mise en place de l’OBU et du RSU (WP 3)

Les deux appareils (OBU et RSU) permettent Mise en place de l’OBU et du RSU et mise en place de la communication entre ces systèmes.

## Spécification de scénarios d’attaques et identification des méthodes et outils offensifs (WP 4)

Mise en place de scénarios d’attaques en fonction de l’implémentation du système OBU-RSU. Mise en place et prise en main d’outils d’attaque.

## Test d’intrusion (WP 5)

Implémentation et réalisation d’un test d’intrusion concret sur les systèmes mis en place durant les phases précédentes.

# Tâches

Ce chapitre décrit les différentes activités qui seront effectuées pour atteindre les objectifs du projet.

## Analyse des communications ITS V2I (WP 2)

* Rédaction du cahier des charges
* Analyse des protocoles ITS basés sur WLAN
* Analyse de l’infrastructure V2I disponible ROSAS

## Mise en place de l’OBU et du RSU (WP 3)

* Mise en place de l'OBU
* Mise en place du RSU
* Mise en place de la communication entre les systèmes
* Intégration du RSU au centre de téléopération

## Spécification de scénarios d’attaques et identification des méthodes et outils offensifs (WP 4)

* Analyse des vecteurs d'attaque sur ITS
* Analyse de la gravité des différentes attaques
* Création d'une matrice de risques des différentes attaques possibles
* Analyse d'outils de pentesting offensifs
* Spécification des attaques réalisables sur les communications V2I

## Test d’intrusion (WP 5)

* Mise en place des outils de pentesting
* Réalisations des attaques
* Rédaction des résultats des différentes attaques

# Dates Clés

|  |  |
| --- | --- |
| * 21.02.2022 (SP-1) | Début du PA |
| * 01.04.2022 (SP-6) | Rendu du document d’analyse des communications ITS |
| * 22.04.2022 (SP-8) | Mise en place complète du système nécessaire à la réalisation des attaques |
| * 13.05.2022 (SP-11) | Document de spécification des scénarios d’attaques et d’identifications des outils offensifs à utiliser |
| * 03.06.2022 (SP-14) | Fin des attaques et du PA et rendu de la documentation |

# Planning

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | SP-1 | SP-2 | SP-3 | SP-4 | SP-5 | SP-6 | SP-7 |  | SP-8 | SP-9 | SP-10 | SP-11 | SP-12 | SP-13 | SP-14 |
| **Analyse des communications ITS V2I** |  |  |  |  |  |  |  | **VACANCES DE PÂQUES** |  |  |  |  |  |  |  |
| Rédaction du cahier des charges |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Analyse des protocoles ITS basés sur WLAN |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Analyse de l’infrastructure V2I disponible ROSAS |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Mise en place de l’OBU et du RSU** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Mise en place de l'OBU |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Mise en place du RSU |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Mise en place de la communication entre les systèmes |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Intégration du RSU au centre de téléopération |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Spécification de scénarios d’attaques et identification d'outils offensifs** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Analyse des vecteurs d'attaque sur ITS |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Analyse de la gravité des différentes attaques |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Création d'une matrice de risques des différentes attaques possibles |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Analyse d'outils de pentesting offensifs |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Spécification des attaques réalisables sur les communications V2I |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Test d'intruision** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Mise en place des outils de pentesting |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Réalisations des attaques |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Rédaction des résultats des différentes attaques |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| Documentation |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

1. https://rosas.center/ [↑](#footnote-ref-2)
2. https://www.rosas.center/fr/projets/teleoperation-de-vehicules-autonomes/ [↑](#footnote-ref-3)