Date 06/04/2023

Défi 01 "Automatisation de la vérification cybersécurité de systèmes cyber physiques"

Journée des chercheurs

Philippe Massonet, Coordinateur Scientifique CETIC
Guillaume Ginis, Chercheur CETIC

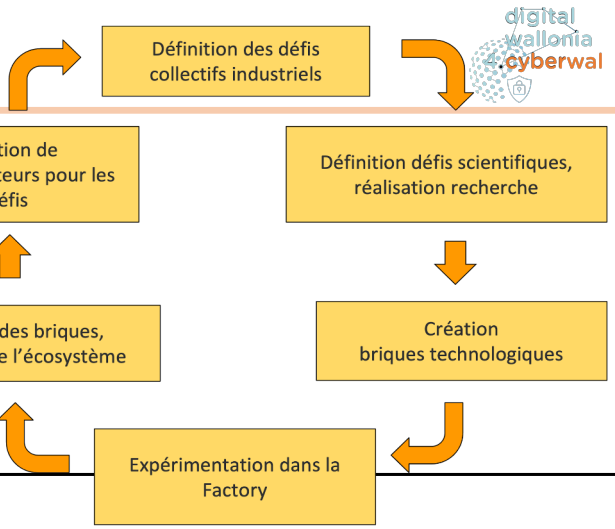
https://cyberwal.be
https://cyberexcellence.be

Agenda

- Cyberexcellence : défis collectifs industriels
- Défi 01 : Automatisation de la vérification cybersécurité de systèmes cyber physiques
- Défi 01 : Etude de cas
- Défi 01 : Résultats du premier groupe de travail
- Related research Project : Cyrus

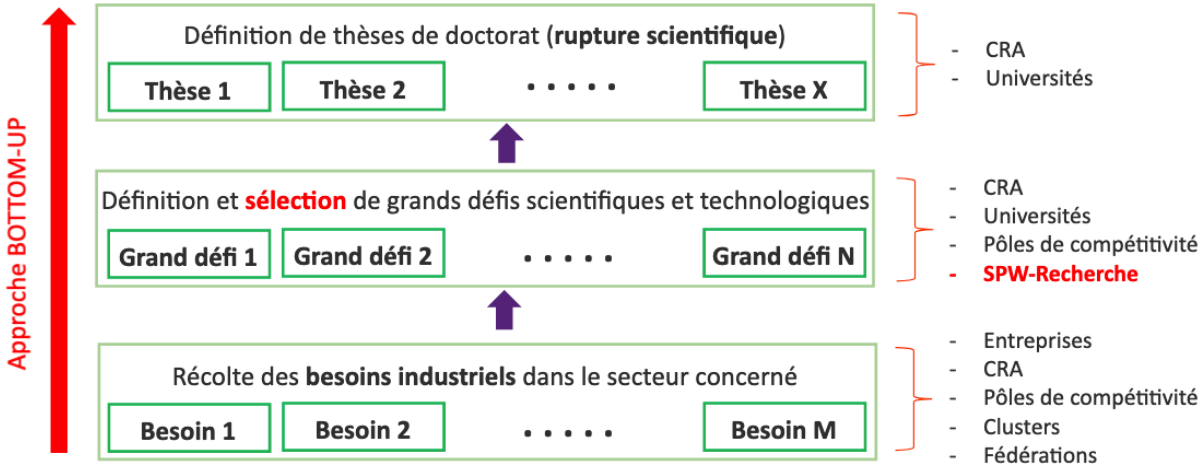
Projet CyberExcellence et Défis Collectifs Industriels

- Projet CyberExcellence
  - Projet de recherche en cybersécurité, 01/01/2022, 18,9 millions de budget)
  - Partenaires : 5 universités + 2 CRA
  - Recherche fondamentale mais **au bénéfice du tissu industriel**: réponds aux besoins des entreprises/administrations
- Défi Collectif Industriel
  - Récolte des besoins industriels dans le secteur concerné
  - Identification des défis Collectif Industrie
- Factory
  - Production de briques technologiques
  - Validées dans des démonstrateurs



Programme Win4Excellence: Objectifs

Wallonie recherche SPW



WP
WP1 : Rendre les systèmes résilients aux cyberattaques : phase de conception.
WP2 : Détection, Réponse, Réaction : Phase Dynamique
WP3 : RGPD et Open data : sécurité à la conception
WP4 : La protection et le partage des données au cœur des préoccupations
WP5 : Laboratoires d'expérimentation, de validation, et d'entraînement
WP6 : Factory et grands défis

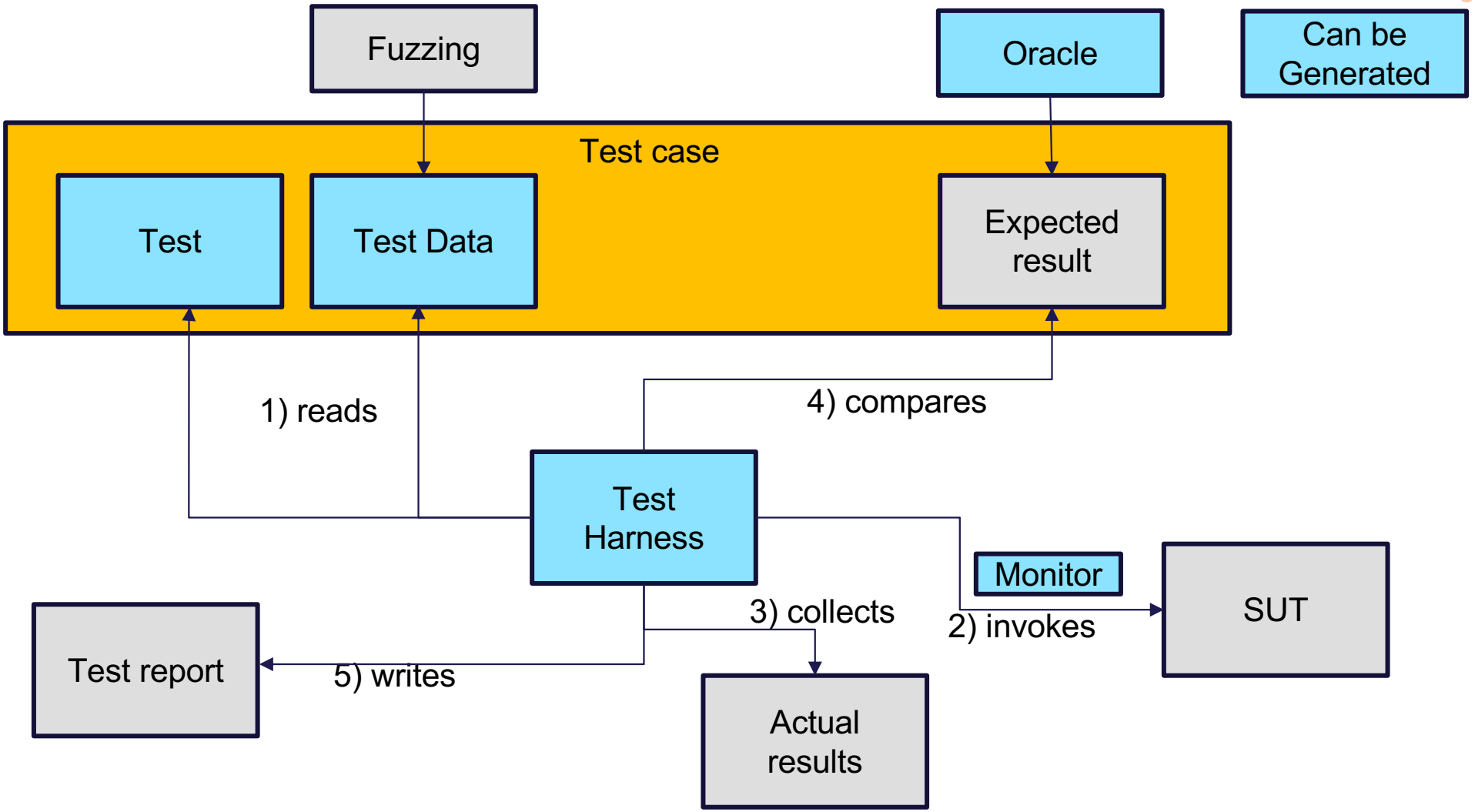
Défi 01 : Automatisation de la vérification cybersécurité de systèmes cyber physiques

- **Résumé du défi:**
  - Tests de pénétration: processus encore très manuel, requiert des experts en cybersécurité
  - Ambition: automatiser (en partie) la création des tests de pénétration pour rendre les tests de pénétration plus accessible par les entreprises (PME, grandes entreprises)

- **Challenges de recherche**:
  - Génération automatique des tests de cybersécurité fonctionnels (architecture de sécurité), utilisation de différentes techniques de génération (à comparer) pour les tests de pénétration:
    - Techniques de fuzzing
    - Génération de tests par mutation génétique
    - Génération de tests à partir de modèles
    - ...
  - Automatisation partielle sous forme d'assistance du processus de création et de la définition des tests de pénétration.
  - « Risk-based testing » pour trouver un meilleur ROI (vulnérabilités/attaques trouvées/budget de test)

Défi 01 : Automatisation de la vérification cybersécurité de CPS

Test Harness

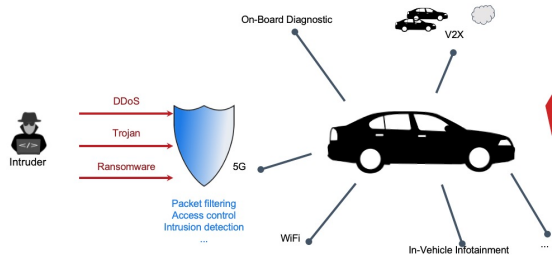


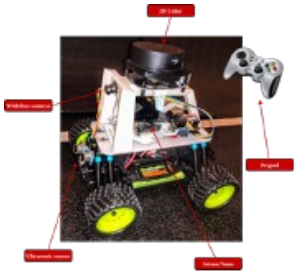
Défi 01 : Automatisation de la vérification cybersécurité de CPS

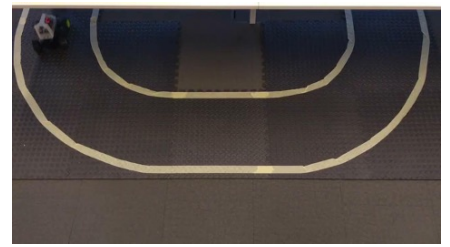
Problèmes de recherche

- Problèmes de recherche
  - UNamur : fuzzing guidé par des algorithmes génétiques (Prof. Xavier Devroey, 1 chercheur)
  - UCLouvain : fuzzing – découverte de protocoles de communication par apprentissage, analyse de malware (Prof. Axel Legay, 2 chercheurs)
  - CETIC : génération de jeux de tests, proposition d'une étude de cas (Philippe Massonet, 2 chercheurs pour 1ETP)

- Expérimentation dans la factory
  - Déploiement d'un système à tester dans une sandbox de la factory
  - Etude de cas :
    - véhicule connecté (V2X)+ centre de gestion de traffic (Cloud)
    - Introduction de vulnérabilités
  - Challenge : tests générés découvrent-ils les vulnérabilités/malware



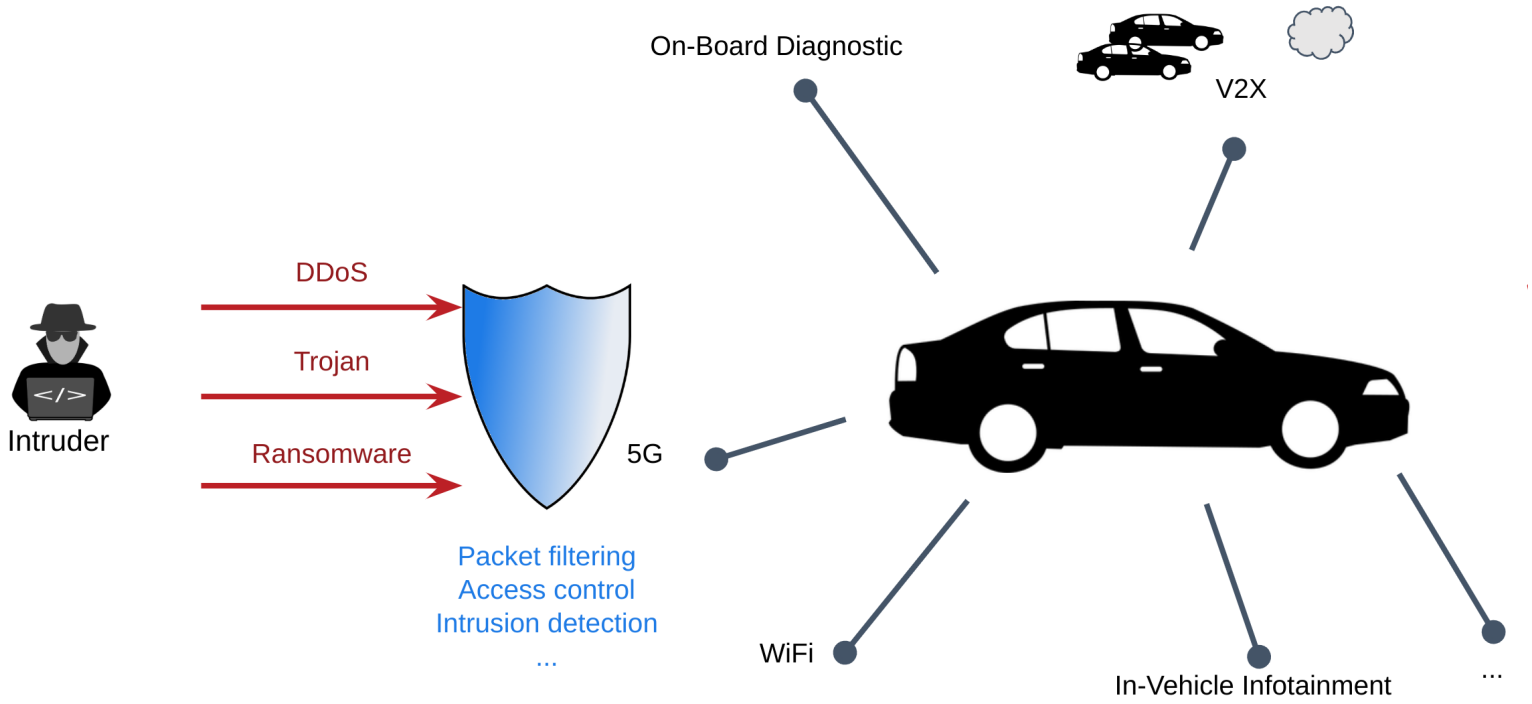




Rover - Donkey Car

Présentation de l'étude de cas – Platooning

Connected vehicles security



- vehicles are getting more and more connected, which increases their attack surface, making them more vulnerable
- increased computing capabilities in cars allow better protection strategies to counter those new threats

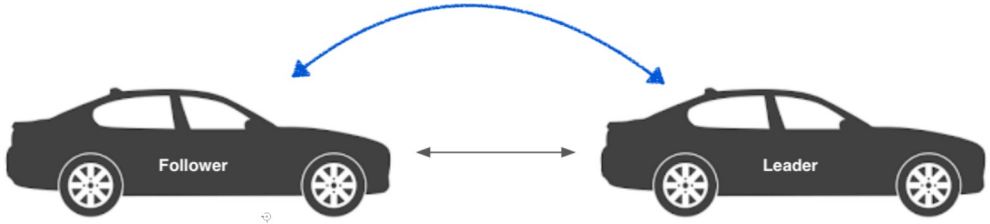
V2X - vehicle to vehicle, vehicle to infrastructure, vehicle to manufacturer, ...

Présentation de l'étude de cas – Platooning

Platooning with connected vehicles

One **leader** vehicle is followed by N other vehicles (« **followers** »).

The vehicles can exchange information on a V2V (vehicle to vehicle) interface and on a V2I (vehicle to infrastructure) interface



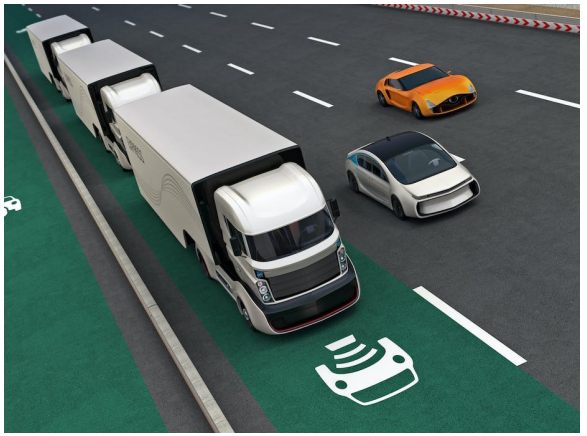
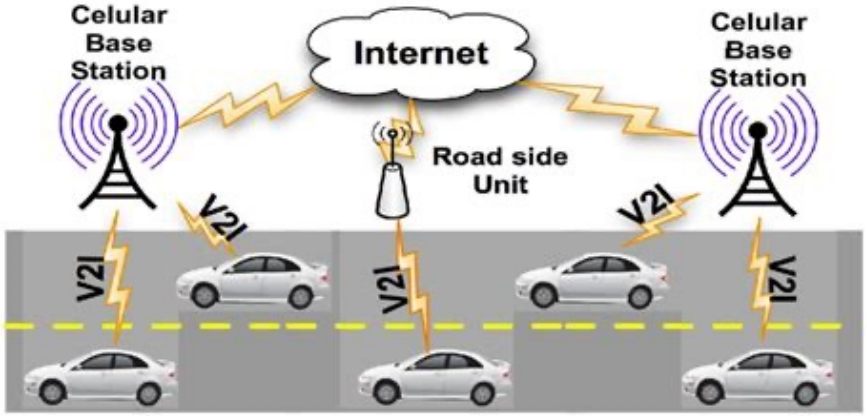
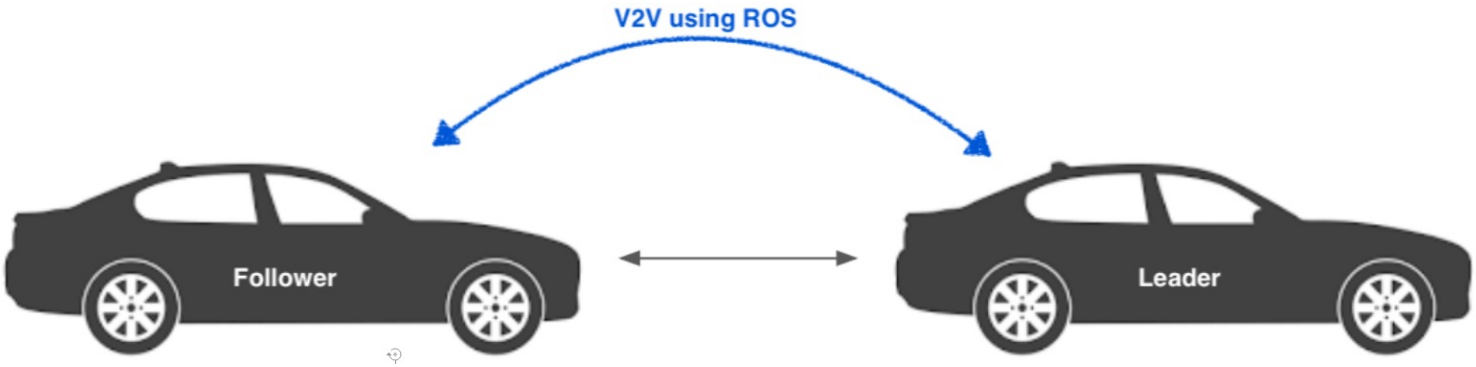


Image source: https://theconversation.com/coming-soon-to-a-highway-near-you-truck-platooning-87748



Présentation de l'étude de cas – Platooning

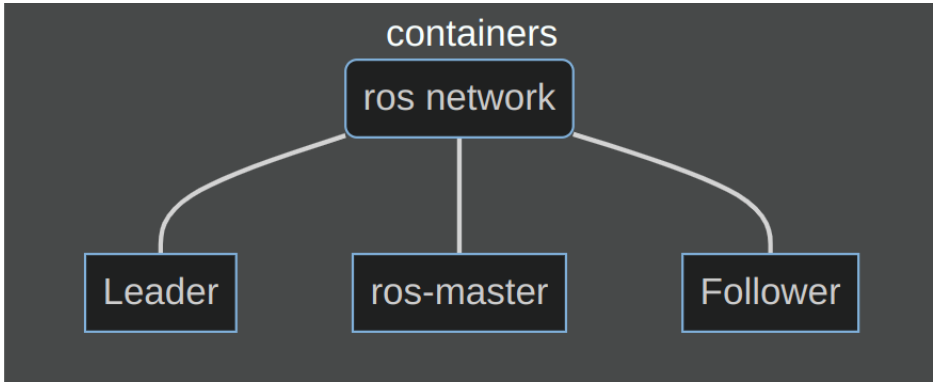
Platooning security vulnerabilities



Any intrusion in the communication can have serious consequences

ROS Protocol v1 :

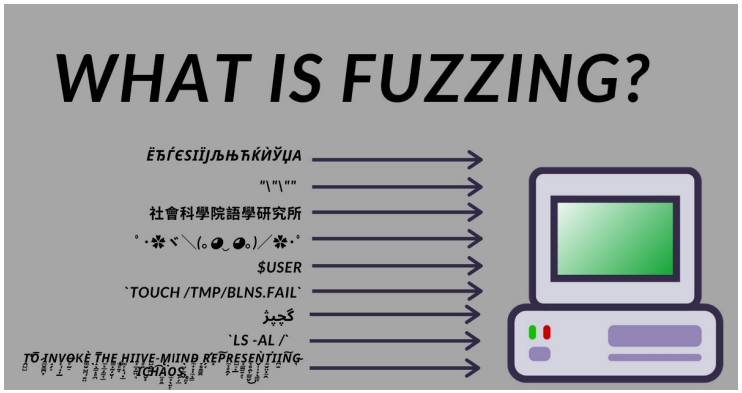
- Publish/Subscribe mechanism with topics
- Use a master to manage communication
- **No encryption**
- **No authentication**
- Basically **No security**

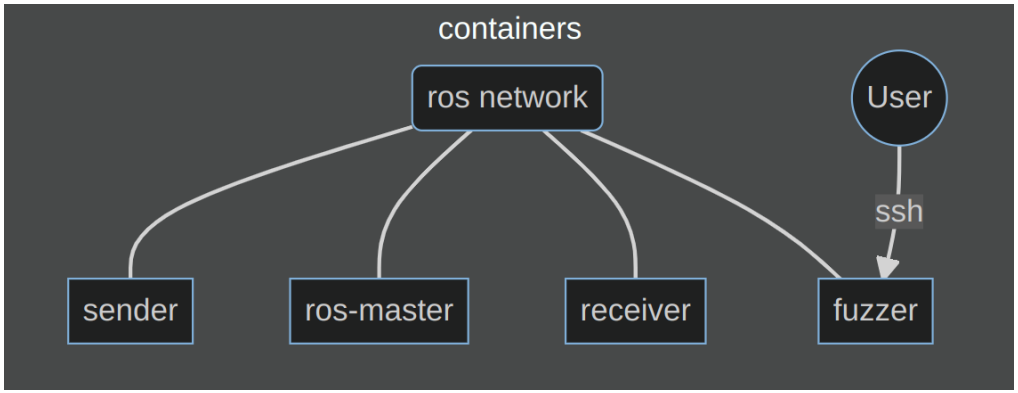


Présentation de l’étude de cas – Platooning

Testing an unprotected system for vulnerabilities and defects

- Fuzzing tests can be performed on the communications between the vehicles.
- Even if the protocol is unprotected, this can reveal defects or vulnerabilities in the follower software
- Example :
  - Random fuzzing and mutation fuzzing on json formatted communications won’t show any effect
  - Grammar Based fuzzing can reveal more vulnerabilities or defects



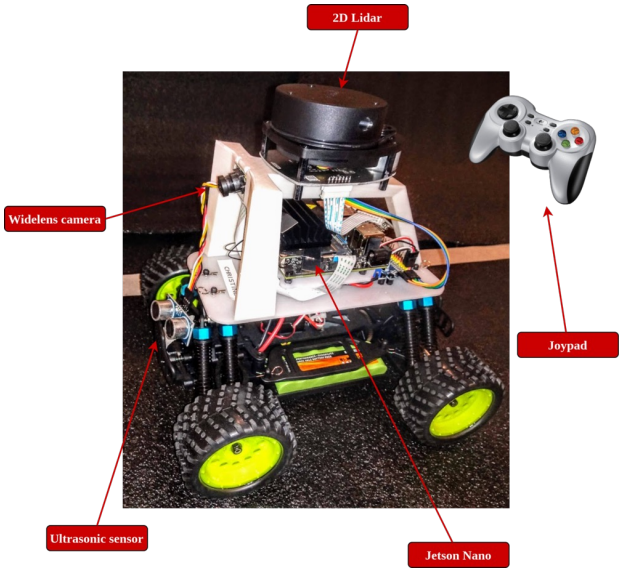


Présentation de l'étude de cas – Platooning

Exploiting Vulnerabilities

The attacker uses this vulnerability to modify the car behavior and create an accident:

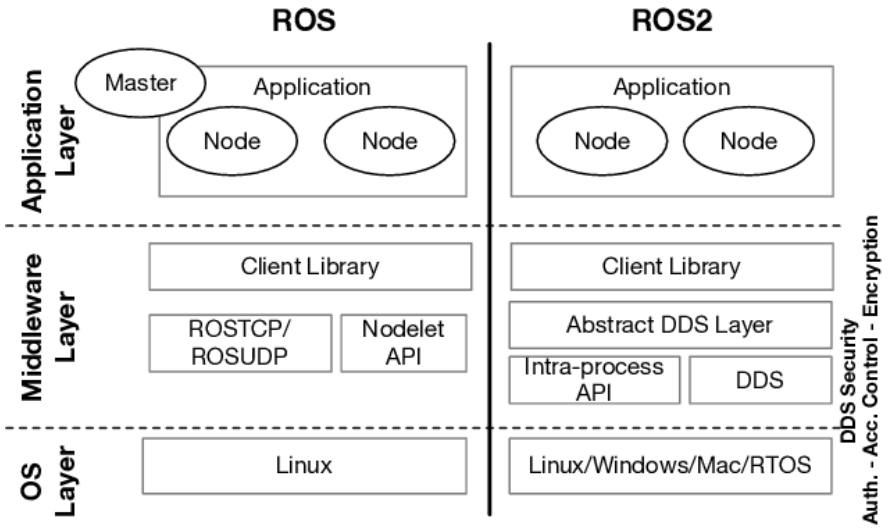
- *forces acceleration, brake, steering*
- *poison camera sensor input*
- *impersonate leader or infrastructure*



https://youtu.be/fZ8goQkyGUs

Présentation de l'étude de cas – Platooning

Testing a **protected** system for vulnerabilities and defects



Mazzeo, Giovanni & Staffa, Mariacarla. (2020). TROS: Protecting Humanoids ROS from Privileged Attackers. International Journal of Social Robotics. 12. 10.1007/s12369-019-00581-4.

ROS2 introduces:

- security - AuthN, AuthZ, communication encryption
- real time
- distributed processing
- resilience & robustness
- ...

Présentation de l'étude de cas – Platooning

Testing a **protected** system for vulnerabilities and defects

2 interesting papers about vulnerabilities discovered on ROS2 and SROS2 (secured ROS2 variant) :

- PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles (source)
- On the (In)Security of Secure ROS2 (source)

2 related CVE :

CVE-2019-19625 Detail

Description

SROS 2 0.8.1 (which provides the tools that generate and distribute keys for Robot Operating System 2 and uses the underlying security plugins of DDS from ROS 2) leaks node information due to a leaky default configuration as indicated in the policy/defaults/dds/governance.xml document.

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 5.3 MEDIUM	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CNA: MITRE	**Base Score:** 7.5 HIGH	**Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

QUICK INFO

CVE Dictionary Entry:
CVE-2019-19625
NVD Published Date:
12/06/2019
NVD Last Modified:
12/13/2019
Source:
MITRE

CVE-2019-19627 Detail

Description

SROS 2 0.8.1 (after CVE-2019-19625 is mitigated) leaks ROS 2 node-related information regardless of the rtps_protection_kind configuration. (SROS2 provides the tools to generate and distribute keys for Robot Operating System 2 and uses the underlying security plugins of DDS from ROS 2.)

Severity CVSS Version 3.x | CVSS Version 2.0

CVSS 3.x Severity and Metrics:

NIST: NVD	**Base Score:** 5.3 MEDIUM	**Vector:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CNA: MITRE	**Base Score:** 7.5 HIGH	**Vector:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

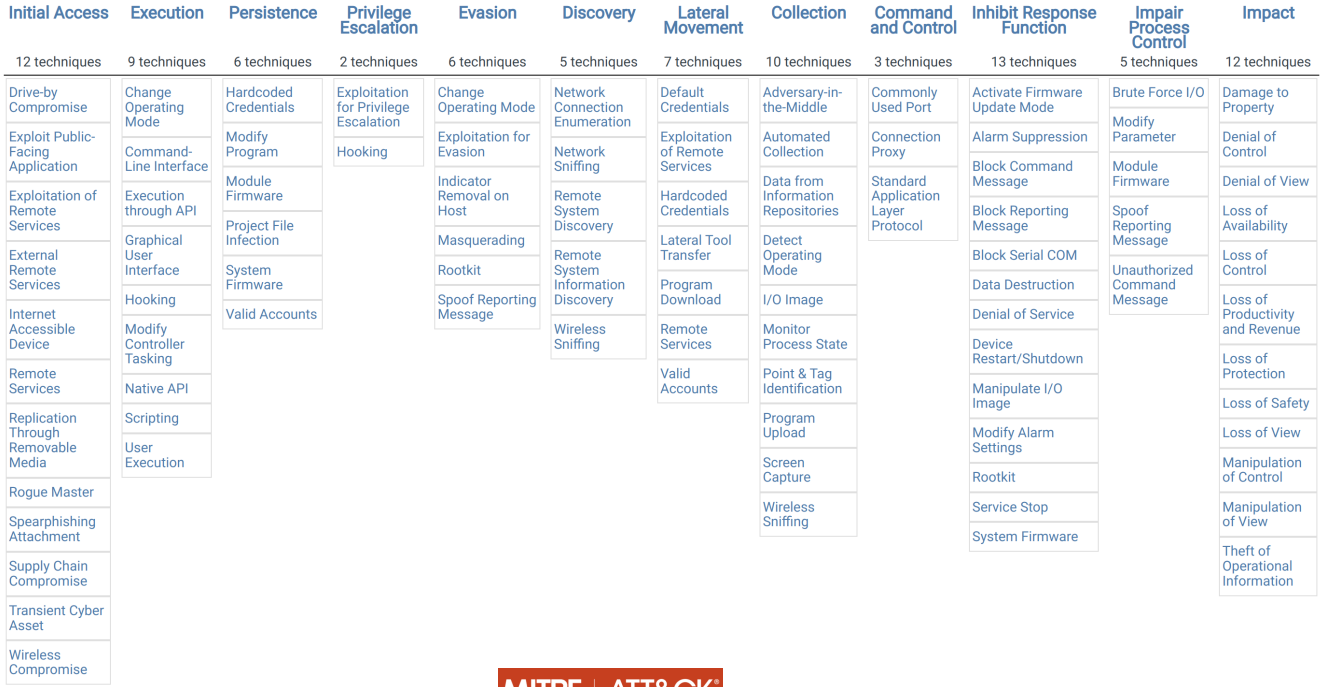
QUICK INFO

CVE Dictionary Entry:
CVE-2019-19627
NVD Published Date:
12/06/2019
NVD Last Modified:
12/13/2019
Source:
MITRE

Présentation de l’étude de cas – Platooning

Testing a **protected** system for vulnerabilities and defects

Remote Access Software (MITRE T1219)
Data Manipulation (MITRE T1565)



Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
12 techniques	9 techniques	6 techniques	2 techniques	6 techniques	5 techniques	7 techniques	10 techniques	3 techniques	13 techniques	5 techniques	12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	I/O Image		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API					Valid Accounts	Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View
Wireless Compromise									Service Stop		Theft of Operational Information
									System Firmware		

MITRE | ATT&CK®

Knowledge base of adversary tactics and techniques based on real-world observations

Résultats du premier groupe de travail

- Les différentes thèses liées au grand défi ont été présentés
- En particulier, Guillaume Nguyen (UNamur), pour sa thématique de recherche, a introduit son besoin de discussion sur les besoins en fuzzing sur CPS des entreprises.

Au niveau des industries :

- ALSTOM partage la même expérience que l'UCL sur les limites du fuzzing et est donc intéressé par leur sujet de recherche. Ils travaillent généralement en white box.
- CYBER COMMAND est plutôt en black-box et est également intéressé par le fuzzing. Ils trouvent le fuzzing aléatoire en black-box plutôt inefficace.
- B12 (consulting) est intéressé de suivre les avancées.
- THALES communication partage l'avis général.

Related Project : CYRUS

Problem: the growing cyber vulnerability of industrial equipment composed of connected cyber-physical systems (CPS)

Solution: development of a demonstrator of a cybersecurity test platform for industrial CPS

Consortium: GUARDIS, Alstom, AISIN, ALX, Cetic, UCLouvain

CPSET project (LiW + Skywin)

Main objectives:

1. Validation and definition of **requirements and specifications**
2. Implementation and validation of the **methodological framework and tools** on a “generic” industrial case
3. Application to several multi-domain **industrial use cases via demonstrator**
4. Validation of the **valorization** scheme and economic model(s)

Related Project : CYRUS

CPSET
Cyber Physical System in Energy conversion & Transportation

digital wallonia cyberwal

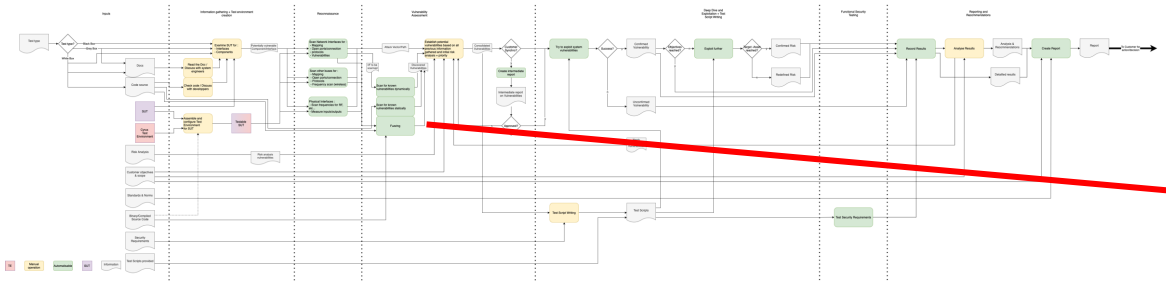
CYRUS

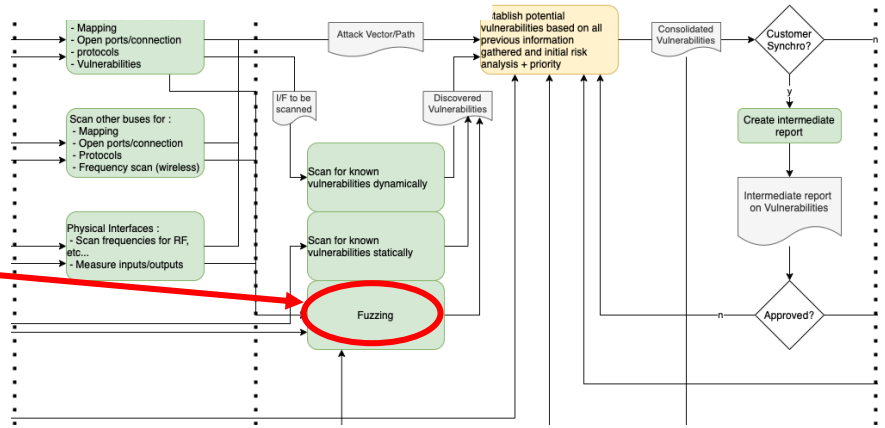
Plateforme de tests de cybersécurité pour systèmes cyber-physiques industriels

CYRUS est un projet de recherche industrielle dont l'objectif est de définir et développer un démonstrateur de plateforme de tests de cybersécurité pour des systèmes cyber-physiques industriels, avec une priorité marquée pour les systèmes critiques en termes de sûreté de fonctionnement.

CETIC · AISIN Europe · Alstom · ALX Systems · Guardis · Plateforme CONTRIBUTE · UCL-ICTEAM

- Includes fuzzing for vulnerability discovery (black or white-box)
- Automate the running of cybersecurity tests on CPS
- Would be interested by fuzzing generated tests to extend its testing capability
- Tests based on automating Framework : RobotFramework (python based)
- Define a generic cybersecurity test procedure

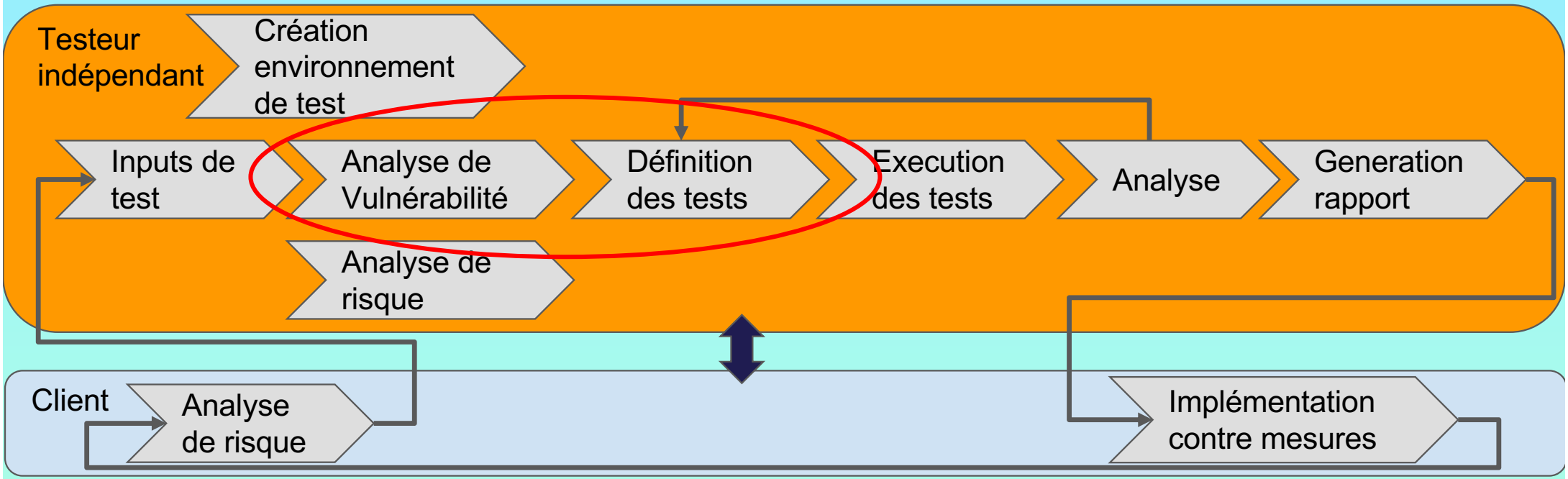




Merci de votre attention

(N’hésitez pas à participer au Défi 1 si la problématique vous intéresse!)

Processus de Tests de Pénétration (https://www.cetic.be/CYRUS-EN)



Classes Outils

Network mapping with scanner | Database Scan | SAST | DAST & WAST | Fuzzing Tools | Wireless attacks | Compliance assessment

Sniffing | MITM | Vulnerability analysis | Firmware analysis | Password attacks | Exploitation tools | Hardware | Forensics

Vulnérabilités, défauts de conception à tester

- Tests
  - Sur un système non protégé
  - Sur un système protégé par une analyse de plausibilité
- Vulnérabilités à tester
  - …

03
Section suivante

Sous-titre de la section

Conclusion

Bulletpoints

1. Section 1
2. Section 2
    - Section 1.1
    - Section 1.2