Colloque IMT

« Gestion de crise et numérique : nouvelles menaces et nouvelles solutions»

31 mars 2022

Posters

Institut Mines-Télécom

Nouvelles approches de gestion des crises

Phd thesis :

Virtual Reality for Cybersecurity

Assistance in the treatment of weak signals

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

CHAIRE CYBER CNI
Sécurité des infrastructures critiques

cyber-cni.fr/

Cybersecurity

- Number of data is exploding, they can come from several sensors
- Algorithms can help to deal with them, but they need human supervision
- How to display huge amount of data in a meaningful way ?

Immersive technologies

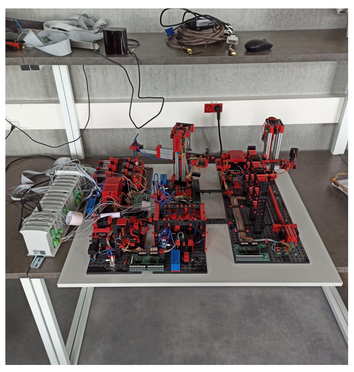
- They offer new ways of interaction and visualization
- They improve operators cyberawareness
- They improve collaboration between operators and decision makers

How to use Immersive technologies for cybersecurity?

- 2 prototypes, Cybercopter and Cubernêtikê: they help the operator investigates data after an alarm has been raised
- They display detected weak signals
- Weak signals: warnings difficult to detect, too incomplete to allow accurate evaluations. In cybersecurity, most attacks disrupt the periodicity of the network but are hidden in the noise.

I. Cybercopter : multivariate temporal data display

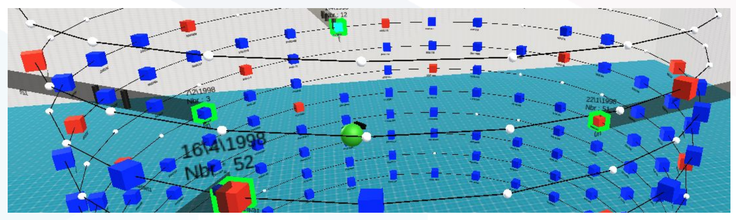
- Data can come from several sources: sensors, Intrusion Detection Software, firewalls
- Helical representations highlight periodic patterns
- Multiple helix allow to display several sensors and their 3D positioning



Sensors

	Timestamp	FIT101	LIT101	MV101
0	28/12/2015 10:00:00 AM	2,427057	522,8467	2
1	28/12/2015 10:00:01 AM	2,446274	522,886	2
2	28/12/2015 10:00:02 AM	2,489191	522,8467	2
3	28/12/2015 10:00:03 AM	2,53435	522,9645	2
4	28/12/2015 10:00:04 AM	2,56926	523,4748	2
5	28/12/2015 10:00:05 AM	2,609294	523,8673	2
6	28/12/2015 10:00:06 AM	2,637158	524,1028	2

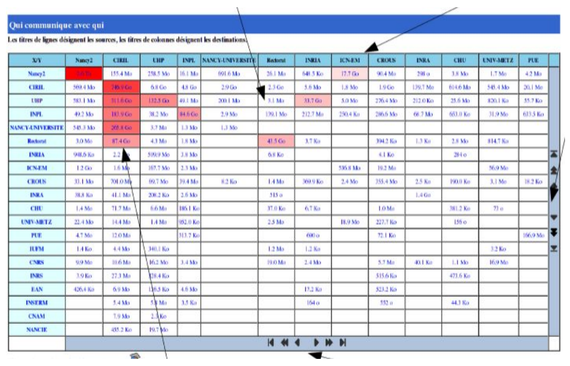
Visualization



- Each cube represents an event
- Cube color depends on its value, blue when low, red when high.
- Helix's period can be changed
- Additional information are displayed using space surrounding the helix

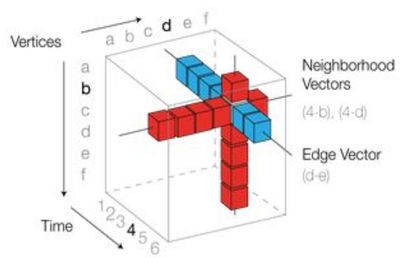
II. Cubernêtikê

- Representation of communications within a network with emphasis on time



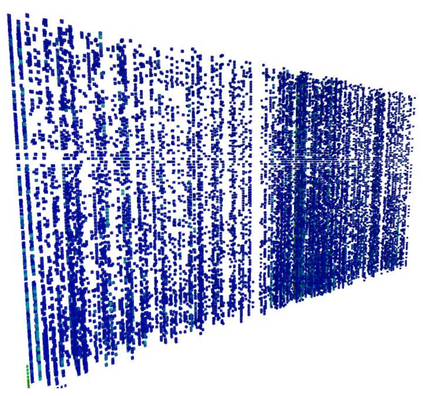
Connection matrix

netMat



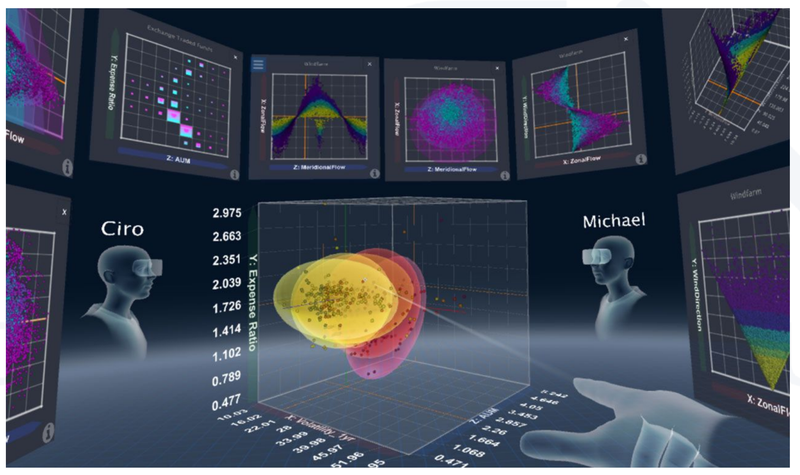
Arnaud Prouzeau

Time axis



III. How to improve interactions with these representations?

- Multimodality:
  - Humans are multimodal creatures, multimodal interfaces improve user performance
  - Use voice as input, e.g. to make a query to a database
  - Use haptic and sound feedbacks as output



Springwise : collaboration in a virtual environment

Contact : nicolas.delcombel@imt-atlantique.fr

School

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Author:

Nicolas Delcombel

Advisors:

Thierry Duval
Marc-Oliver Pahl

Partners

AMOSSYS
BNP PARIBAS
La banque d'un monde qui change
AIRBUS DEFENCE & SPACE

CHAIR OF CYBER CNI
Critical National Infrastructures

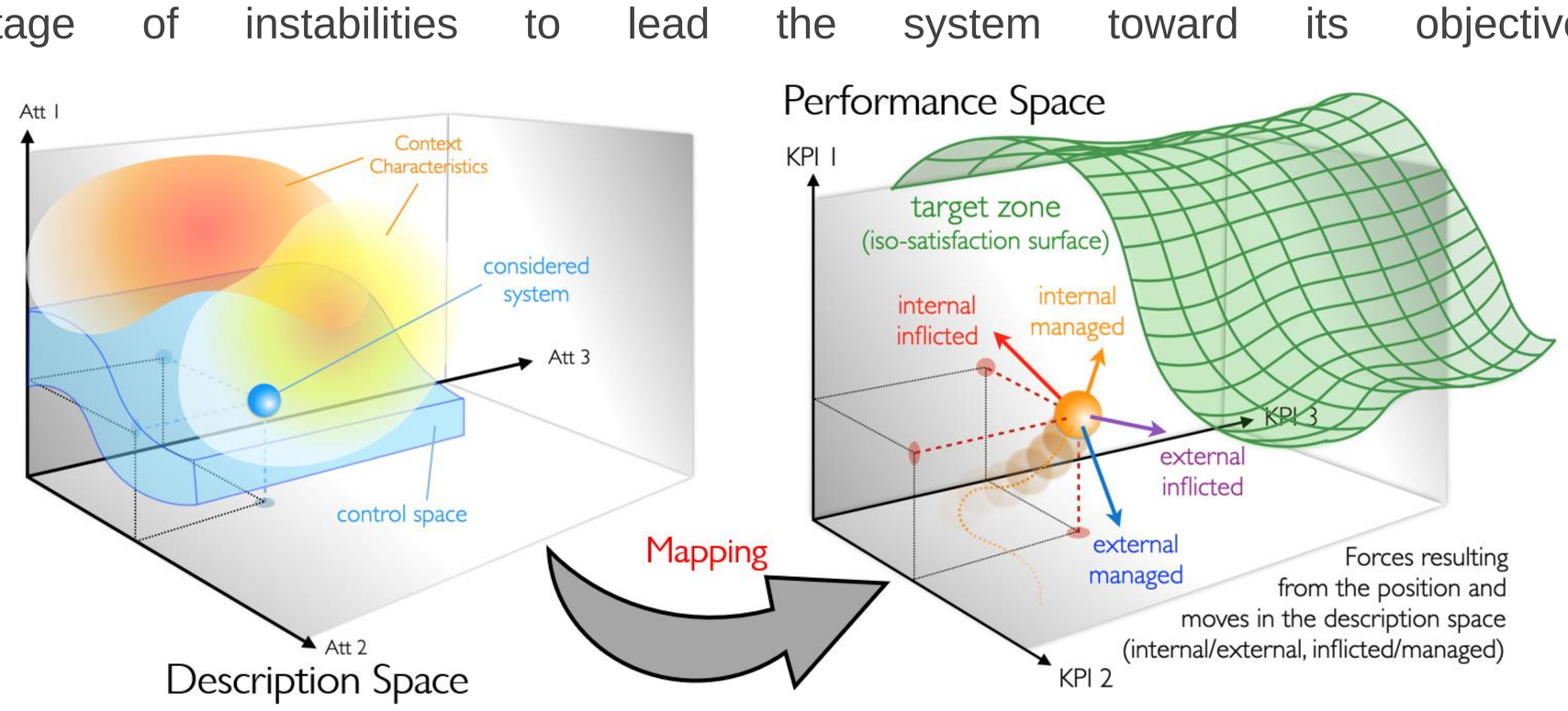
This poster was made at the chaire Cybersecurity for Critical Networked Infrastructures (Cyber CNI) | https://cyber-cni.fr/ | Our monthly cybersecurity speaker series https://talk.cybercni.fr/ | Our science blog https://future-iot.org/

Institut Mines-Télécom
IMT Atlantique Bretagne-Pays de la Loire École Mines-Télécom
TELECOM Paris
TELECOM SudParis
AIRBUS AMOSSYS BNP PARIBAS La banque d'un monde qui change
EDF NOKIA Bell Labs SNCF PÔLE D'EXCELLENCE CYBER
UNION EUROPÉENNE UNIANIEZH EUROPA L'Europe s'engage en Bretagne
Région BRETAGNE

The Physics of Decision (POD)

Intelligent decision technology system inherited from physics for risk and crisis management

Managing multi-criteria systems in which instability is almost ubiquitous induces the systems and their performance to adapt. In this context, management entails (i) recognizing the components which play key roles in the system instabilities and (ii) taking advantage of instabilities to lead the system toward its objectives.



Physics of Decision spaces

Laboratory

Authors

Nafe Moradkhani
Frédérick Benaben
Benoit Montreuil
Matthieu Lauras
Thibaut Cerabona
Clara Le Duff
Julien Jeany
Jean-philippe Gitto

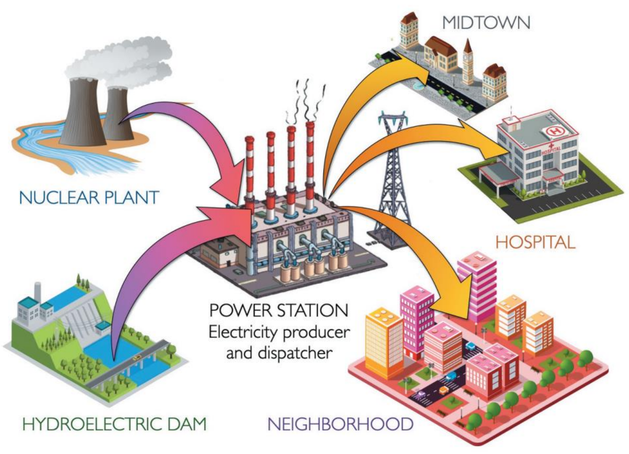
Partners

Multidisciplinary approach in Decision Support System

- **System establishment and characterization (Modelization):** Collecting and describing the system intentions (KPI), system's associated contextual parameters, system's potentials (Risks and Opportunities)
- **System vulnerability and sustainability identification (Preference):** Detailed assessment of the investigated system through sensitivity analysis (e.g., simulation campaign runs, Artificial Neural Networks (ANN), and clustering) to infer the correlation matrix between the potentials (internal and external) and the intended KPIs
- **Strategy exploration (Intelligence):** Using the optimization algorithms, notably the heuristic approach, to offer the most desirable decisions to lead the system toward its objectives

Application Domains

Energy Distribution



Traffic Management

Pandemic Management

Air pollution Management

Contact : nafe.moradkhani@mines-albi.fr

March 2022 Colloque IMT « Gestion de crise et numérique »

La cellule de crise du futur

Connaissance de la situation et prise de décision en réalité virtuelle

La réponse à une crise nécessite une connaissance précise de la situation partagée par les équipes d'intervention, pour prendre les décisions et piloter les opérations. Pourtant, ces éléments présentent actuellement plusieurs défauts. Le projet présenté ici propose d'utiliser la réalité virtuelle pour proposer une cellule de crise virtuelle et améliorer ces aspects.

Parties Prenantes

IMT Mines Albi-Carmaux
École Mines-Télécom

Auteurs

Aurélie Congès

Frédérick Benaben

Col. Jacob Graham

Matthieu Lauras

Partenaires

PennState

IMMERSIVE FACTORY

Report One

La Région Occitanie Pyrénées - Méditerranée

L'EUROPE S'ENGAGE L'OCCITANIE AGIT

UNION EUROPÉENNE

Projet cofinancé par le Fonds Européen de Développement Régional

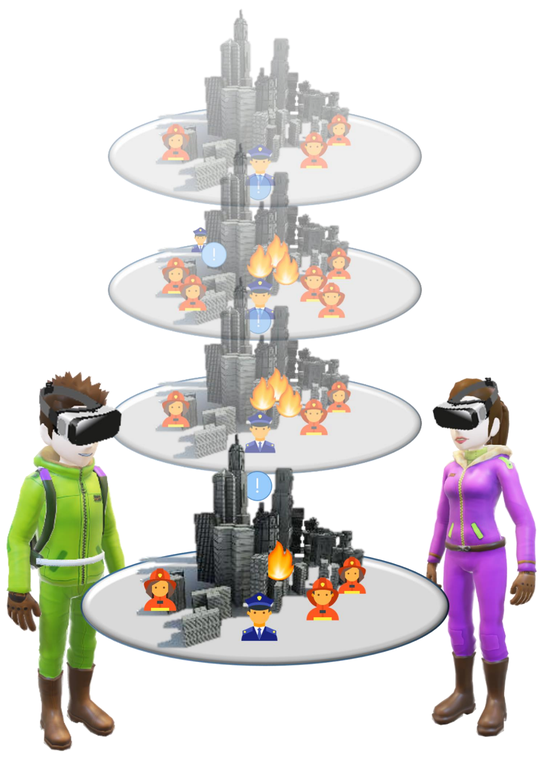
Reproduction de la crise sur la carte 3D

Connaissance de la situation

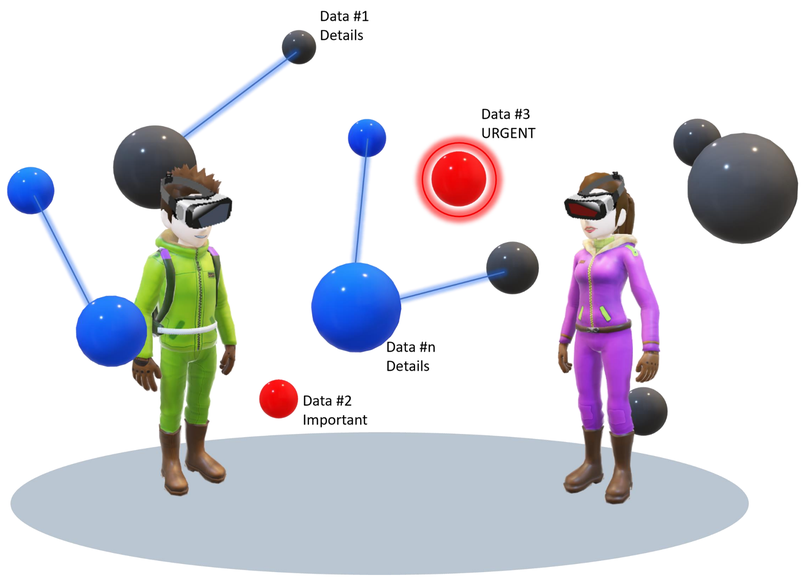
- **Visualiser la crise** – Reproduction en temps réel de la crise et de son évolution sur une carte 3D à l'aide de capteurs pour visualiser les acteurs, ressources, risques et dangers
- **Mise à jour** – La cellule de crise est mise à jour en temps réel via des capteurs (présence, fumée, réseaux sociaux…)
- **Adopter plusieurs points de vue** – Carte interactive que l'on peut tourner, déplacer ou zoomer pour adopter différents points de vue, de la vue de dessus à la vue 1ère personne
- **Multijoueur** – Possibilité pour plusieurs utilisateurs de se rejoindre dans la cellule de crise virtuelle et de communiquer même s'ils ne sont pas physiquement au même endroit

Prise de décision

- **Schéma de réponse** – La cellule de crise est connectée à un système d'aide à la décision pour déduire et visualiser un schéma de réponse à la crise
- **Connexion avec le terrain** – Les acteurs sur site peuvent recevoir des informations ou des instructions de la cellule de crise
- **Anticipation** – Visualisation de l'évolution de la situation basée sur le schéma de réponse et sur des prévisions (météo, trafic, opérations à mener…)
- **Expérimentation** – Essai de mise en place de solutions potentielles et visualisation des conséquences afin de les valider ou non
- **Immersive Analytics** – Évolution des utilisateurs au milieu des données et utilisation de métaphores spatiales pour visualiser et comprendre des données complexes



Visualisation des situations anticipées



Evoluer au milieu de la donnée

Implémentation

- **Flash** – Scannez le QR code pour voir une démonstration du prototype

La cellule de crise virtuelle

Contact: aurelie.conges@mines-albi.fr

Colloque IMT « Gestion de crise et numérique »

Mars 2022

RISK MANAGEMENT AND DISASTER RESPONSE IN THE OIL AND GAS INDUSTRY:

SET-UP, DESIGN AND IMPLEMENTATION OF INNOVATIVE AND INTEROPERABLE SOLUTION FOR A MOBILE FIELD HOSPITAL (MFH) DEDICATED FOR OIL AND GAS INDUSTRY.

Authors

Nimisingha Jacob AMAKAMA
Gilles DUSSERRE
Axelle CADIERE

Partners

Université de Nimes

PTDF Nigeria

Campus France

Overview

Disasters in intricate environments requires response that is adapted(promptness, deployment and retrieval etc.) to the needs of the affected.

MFH-A mobile health facility capable of rapid deployment and expansion to meet immediate emergency needs.

Because of the prevalence and maturity of available tools, the use of a standard modelling language such as Business Process Model and Notation (BPMN) is recommended to define procedures and processes.

Fig.1: Disaster Response Plan

Objectives

- Design and innovative and interoperable MFH for the oil and gas industry,
- Propose most appropriate set up with best functionality, deployment and transportation options,
- Identify driving features for MFH dedicate for the oil and gas industry,
- Recommendation for training and best practices guidelines.

Research Questions

- What factors drives disasters/accidents episodes during drilling and production operations?
- What are the common hazards in the oil and gas industry?
- Is the interoperable MFH dedicated for the oil and gas industry sustainable?

Methodology

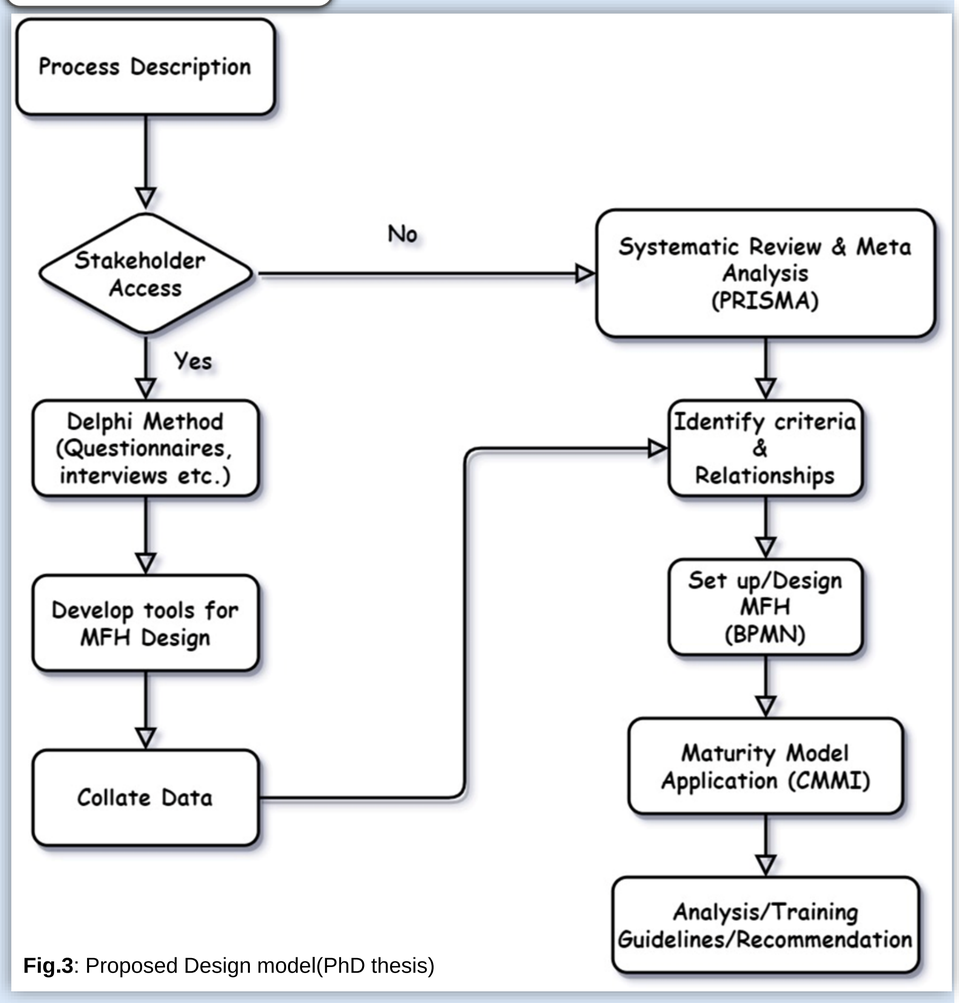


Fig.3: Proposed Design model(PhD thesis)

Expected Outcomes

- Innovative set-up/design and orientation of the most appropriate components for the MFH dedicated for the oil and gas industry,
- A detailed guideline to support users training, in order to minimize associated mobile field hospital deployment/retrieval challenges,
- Recommendation of innovative mobile field hospital wastewater treatment technology.

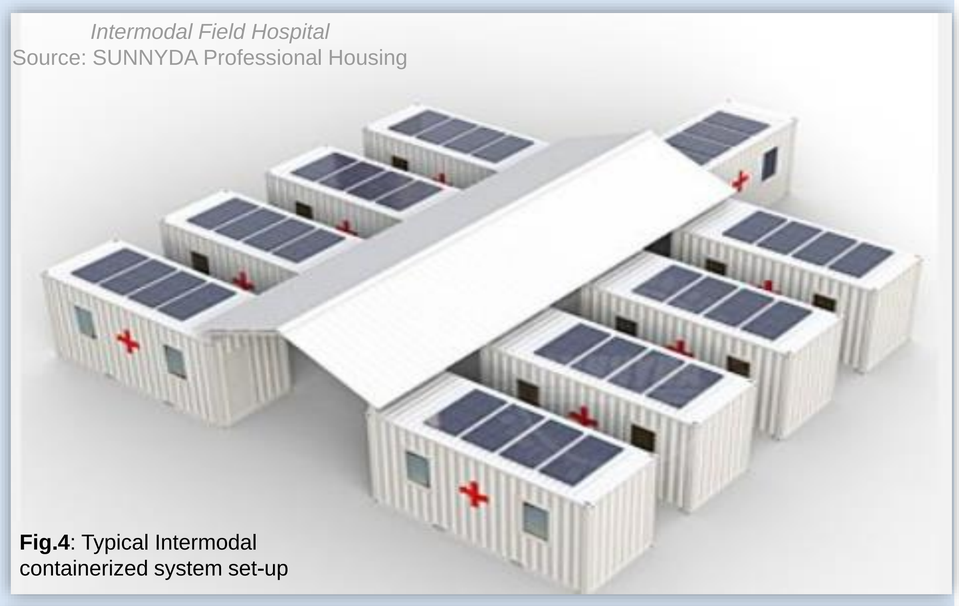


Fig.4: Typical Intermodal containerized system set-up

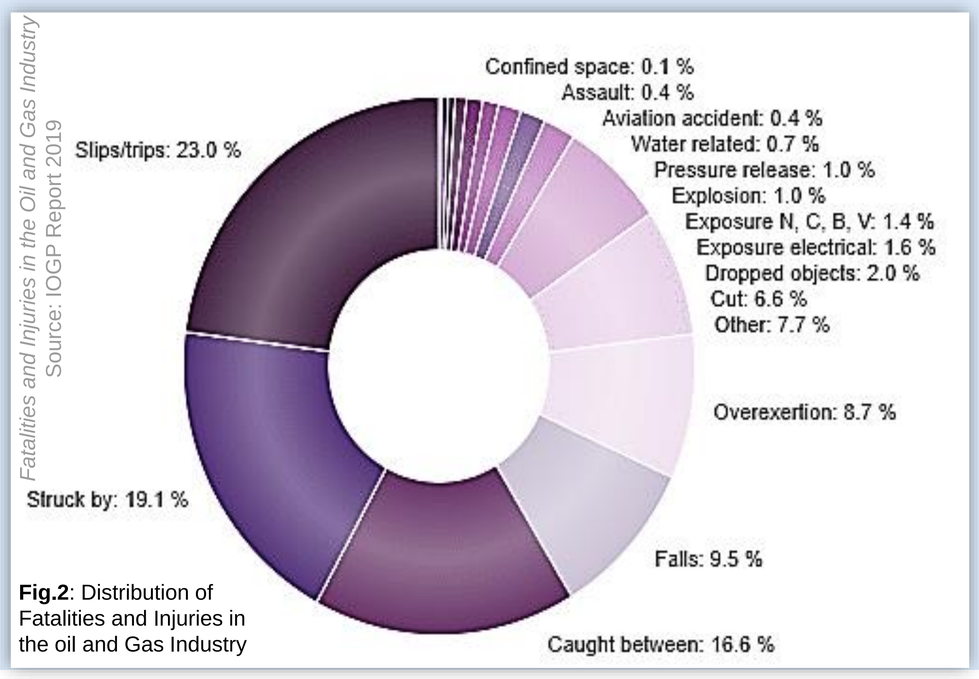


Fig.2: Distribution of Fatalities and Injuries in the oil and Gas Industry

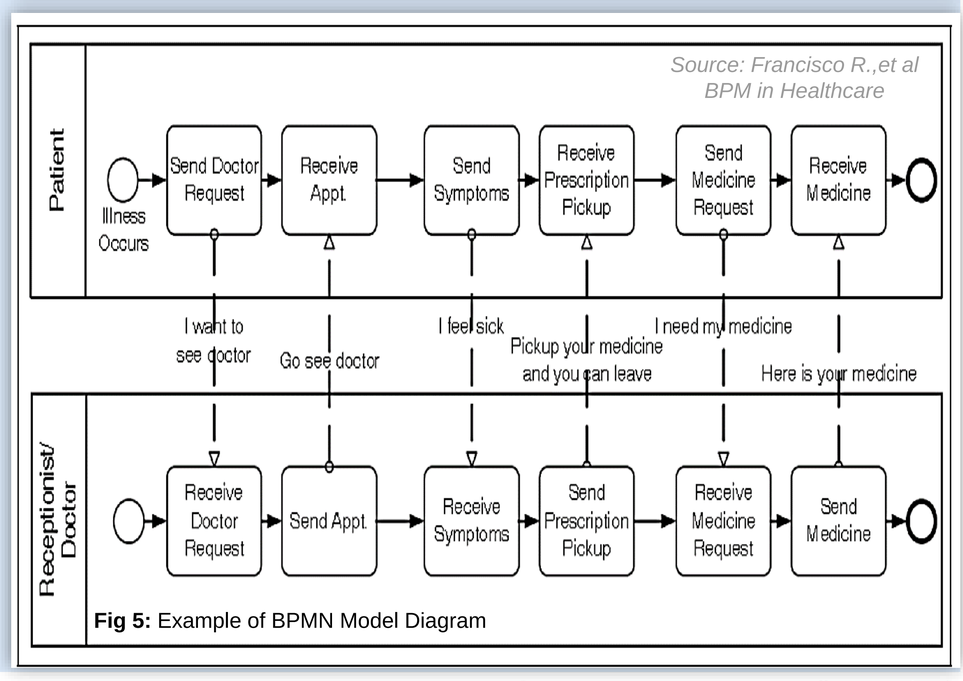


Fig 5: Example of BPMN Model Diagram

Contact : nimisingha.amakama@mines-ales.fr

RISK MANAGEMENT AND DISASTER RESPONSE
HEALTH SECTOR:

Disease Outbreaks Prediction and Monitoring Modelling using a variable Tool of Remote Sensing and GIS; An integral study of Disaster preparedness and Response in Disaster management.

Authors

Nanlok Henry NIMLANG

Gilles DUSERRE

Sandrine BAYLE

Kivanc ERTUGAY

Partners

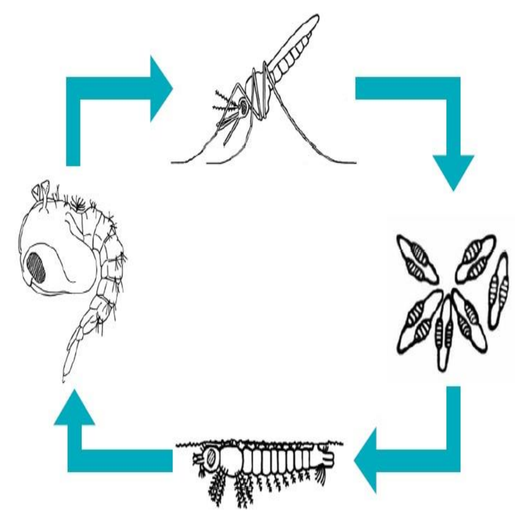
Université de Nimes

PTDF Nigeria

Campus France

CONTEXT:

- **Biological Disasters:** Scenarios causing diseases, disabilities or death on a large scale among humans, animals and plants due to toxins or disease caused by living organisms or their products and hence creating human, property and environmental loses.
- **Diseases Outbreaks:** Nigeria has the highest malaria endemicity contributing 27% of the world's malaria burden.
- **Disease Prediction Modelling:** Developing and Modelling realistic Diseases Predictive Models for Nigeria Malaria Elimination Control Program to aid in effective, sustainable and efficient management processes.
- **Malaria Elimination Strategies:** Holistic Assessment, Analysis and Evaluation of the Malaria Elimination Successes, Failures and Strategies used in Nigeria's Malaria Control Programmes is important in achieving Malaria Elimination in the Country.

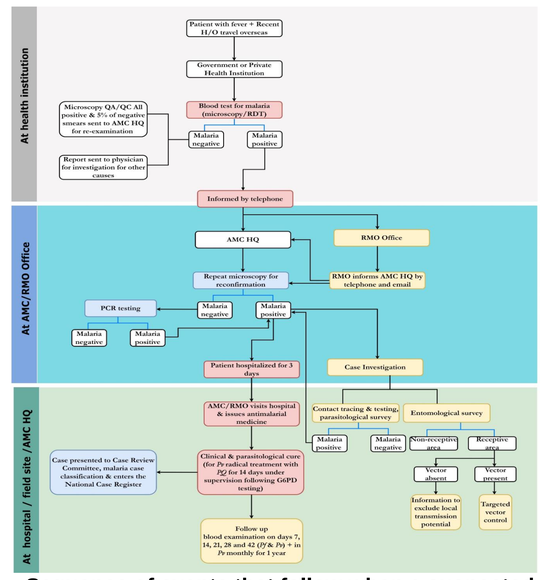


Anopheline mosquito life cycle

Source: WHO, 2014

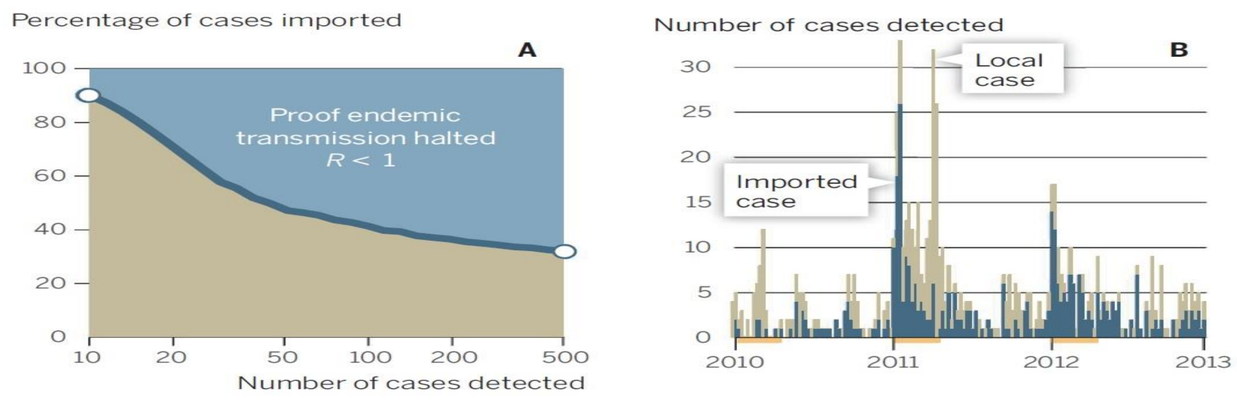
RESEARCH OBJECTIVES:

- **Holistic Assessment, Evaluation and Analysis** of the Malaria Elimination Successes, Failures, Strategies and Research Gaps in Nigeria using World Health Organization's Malaria Elimination Guidelines with the view of correcting its lapses.
- **Spatio-temporal Analysis and Modelling** of Malaria Incidence and Prevalence trends in Nigeria.
- **Evaluation, Analysis and Modelling** to of Malaria Incidence and Prevalence using Machine Learning to examine the Hospital Case Scenarios.
- **Developing** and **Evaluating a realistic** Models for Nigerian Malaria Elimination Programmes for an effective, efficient and sustainable management decision making tool.



Sequence of events that follow when a suspected malaria patient presents at a health institution in either the public private sector in Sri Lanka

Source : Premaratne et al., 2019

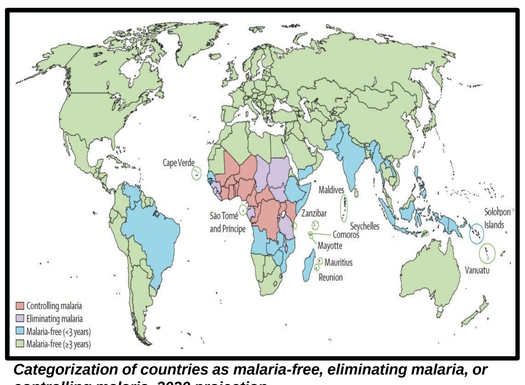


Source : Churcher et al., 2014

Tracking malaria transmission. (A) The percentage of imported cases required to confirm that endemic malaria transmission has been halted. If the percentage of imported cases is greater than the solid dark blue line (blue area), there is statistical evidence that malaria is no longer endemic. The tan areas show where the hypothesis that *R* ≥ 1 cannot be rejected, either because there is insufficient evidence or because endemic transmission is ongoing. (B) The weekly incidence of malaria cases investigated in Swaziland. All cases are likely to be falciparum malaria (*9*). Orange lines on the *x* axis indicate the high-transmission season. (C) Estimates of the reproduction number *R* for each season in Swaziland, with shaded area indicating 95% credibility intervals.

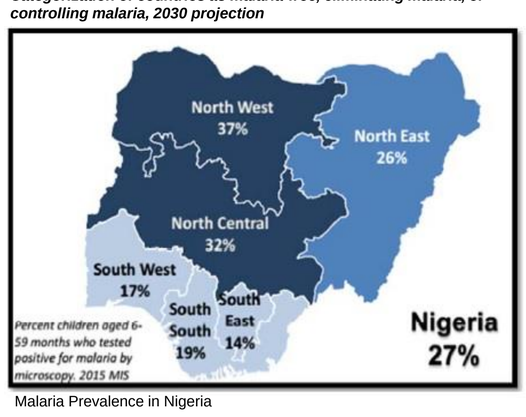
EXPECTED OUTCOMES:

- **Spatio-temporal Analysis of the Malaria Scenario** to evaluate the Malaria Control and Elimination Strategies in Nigeria.
- **Effective, Sustainable and Efficient use of Realist Models** for the trends of Malaria Incidence and Prevalence Hospital Cases in Nigeria.
- **Develop a Structural Framework** to for the Malaria Control and Elimination programme for effective and efficient management of the disease.
- Recommendations for achieving the **World Health Organization** Malaria Control/Elimination for Certification in Nigeria.



Categorization of countries as malaria-free, eliminating malaria, or controlling malaria, 2030 projection

Source: WHO, 2010



Malaria Prevalence in Nigeria

Source: WHO, 2016

Contact : Nanlock.Nimlang@mines-ales.fr

Colloque de l'Institut Mines Télécom Paris, 2022.

ARTIFICIAL INTELLIGENCE IN CRITICAL INFRASTRUCTURES:

AI PARADIGM FOR ENHANCED CYBER ATTACK DETECTION IN CRITICAL INFRASTRUCTURES

Authors

EMMANUEL Song Shombot
Gilles DUSSERRE
Nicolas DACLIN
Marc OLIVAUX

Partners

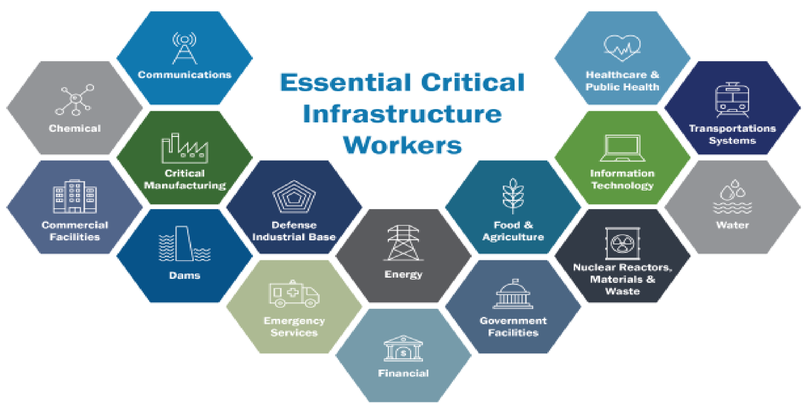
Université de Nimes

PTDF Nigeria

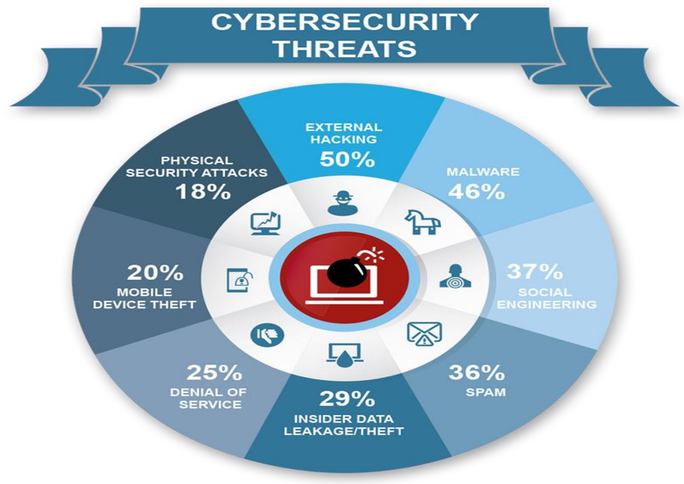
Campus France

CONTEXT:

- **Artificial Intelligence:** Computer Systems capable of simulating human intelligence when performing tasks.
- **Critical Infrastructures:** Critical infrastructures such as health care systems or the oil and gas industry.
- **Cyber Attack Modelling using AI tools:** Simulation of sophisticated cyber-attacks and using AI tools for knowledge building and resilience test
- Need to **prepare, detect, respond and recover** from any form of Cyber attack: **Cyber Resilience**



Filed Critical Infrastructure
Source : : Security Magazine



Data breaches
Source :Security Magazine

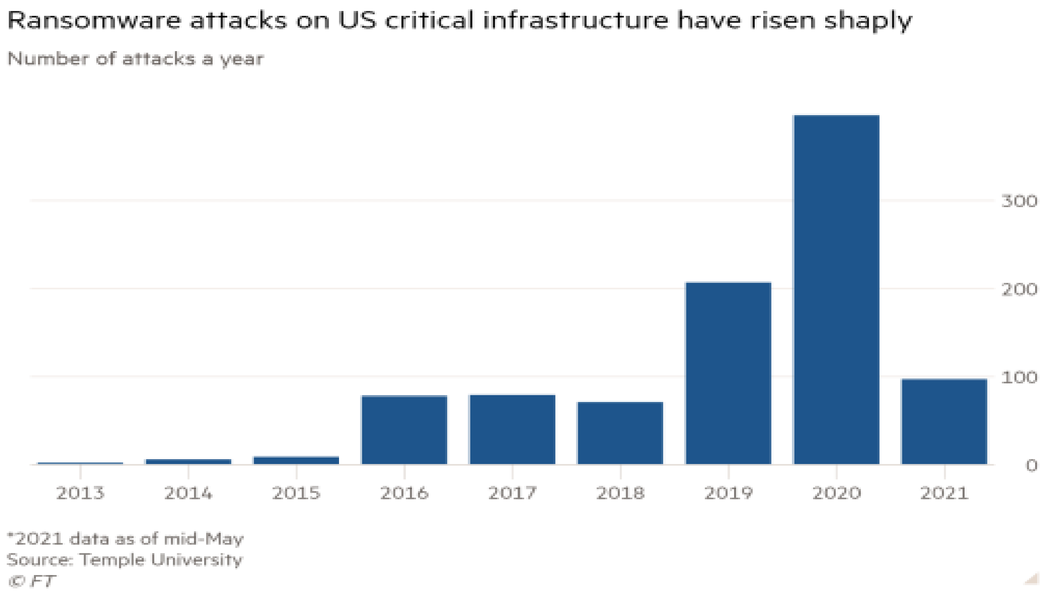
RESEARCH QUESTIONS:

1. What are the commonly targeted cyber assets in critical infrastructures? (eg. medical records, software, supply chain systems & storage media)

***2.* How will AI tools application enhance security administration?** (Detection, Prediction Modelling, Assessment, testing, prevention, response, recommendations and training)

RESEARCH OBJECTIVES:

- **Review** state of the art literature on AI and ML.
- **Design** a robust database system and populate it with simulation datasets.
- **Train** the model for cyber threat detection in critical infrastructures.
- **Model Testing** by carrying out series of Cyber-attacks to determine detection and prediction accuracy of the model.



CRAF
Source : NIST/ISO27001

Cyber assets
Source : MFH world

Data breaches
Source :Security Magazine

Technical setup
Source: Public Safety

RESEARCH OUTCOMES:

- **Designing a Database** for Cyber attacks
- **Use AI tools** for behaviour prediction modelling
- **Lessons Learnt** from each successfully implemented attack
- **Evaluation of the Model** and knowledge management

Contact : emmanuel_song@yahoo.ca

FERUARY 2022 Ecole des Mines D'Ales

CYBER SECURITY IN THE HEALTHCARE SYSTEM:

EVALUATION AND ASSESSMENT OF CYBER SECURITY READINESS IN MOBILE FIELD HOSPITAL'S RESILIENCE

Authors

Nasir Baba AHMED
Gilles DUSSERRE
Nicolas DACLIN
Marc OLIVAUX

Partners

Université de Nimes

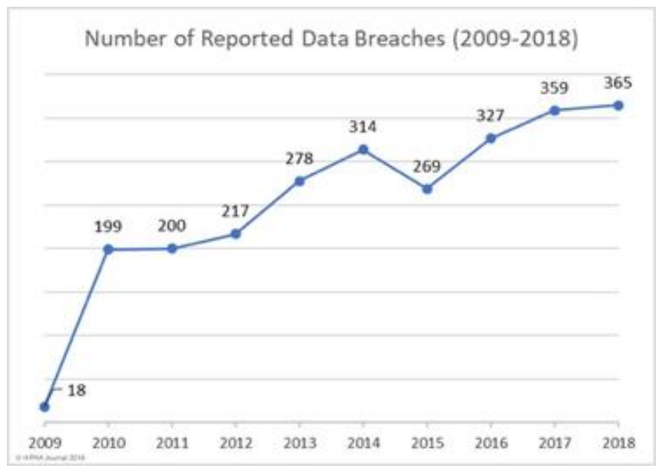
PTDF Nigeria

Campus France

CONTEXT:

- **Mobile Field Hospital:** A subsystem of a traditional hospital deployed to deliver medical services during emergencies
- **Use of IT/Cyber Assets:** Support users/stakeholders in efficient management of processes and patients (e.g. barcode-bracelets, tablets, network devices)
- **Health sector as a target:** Cyber-attacks rising on healthcare/systems today for Data, Disruptions and people's lives
- Need to **prepare, detect, respond and recover** from any form of Cyber attack: **Cyber Resilience**

Filed hospitals
Source : MFH world



Data breaches
Source :HIPAA Journal

RESEARCH QUESTIONS:

1. Are the Mobile Filed Hospitals SAFE from of Cyber-attack? (e.g. medical devices, patient data transfer & storage)

***2.* Which processes can be used in improving the Cyber resilience of the MFH?** (Assessment, testing, prevention, response, recommendations and training)

RESEARCH OBJECTIVES:

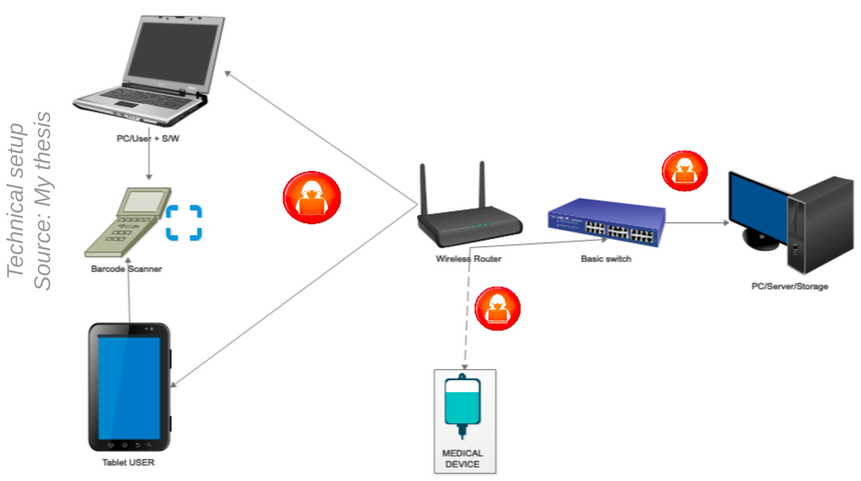
- **Evaluation** of the **Cyber Resilience** in MFH's cyber infrastructure, and its organizational operations.
- **Cyber Resilience Assessment Model** (MFH-CRAF) to assess organisational and technical aspects in MFH - offline evaluation
- **Scenario based Technical Penetration tests** to support data practically and scientifically on MFH's cyber assets - online/active evaluation
- **Cyber Resilience Strategy** and **vulgarised implementation** process, sustainable for the MFH infrastructure.

Function	Category	Subcategory	More Information	Current Practice	Predicted Practice
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the MFH's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	ID.GV-1: MFH cybersecurity policy is established and communicated	Is there a cybersecurity policy implemted for the MFH use of its cyber assets?	1.0	2.0
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and other Stakeholders	Are the cybersecurity practices the same and shared with other stakeholders?	1.0	2.0
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	Are the cybersecurity practices the same and shared with other stakeholders?	1.0	2.0
		ID.GV-4: Governance and risk management processes address cybersecurity risks	Are the risk management processes addressing the issues of cyber risk?	1.0	1.0
	Category Maturity Score			1.0	1.8

CRAF
Source : NIST/ISO27001

Cyber assets
Source : MFH world

Cyber assets
Source : MFH world



Technical setup
Source: My thesis

RESEARCH OUTCOMES:

- MFH **CRAF Model** for offline evaluation
- **Scenario Repository** for Technical/Physical Tests
- **Structured Approach** to usage of CRAF & Cyber TTX
  - (including: Planning & execution of Cyber drills/Exercises)
- Recommendations for **CRAF implementation**
- Recommendations for **CRAF Guidelines/Awareness/Training**
- **Penetration Test** implementation & results analysis

Contact : nasir-baba.ahmed@mines-ales.tr

FEBRUARY 2022 Ecole des Mines D'Ales

CYBER-PHYSICAL INTRUSION DETECTION DRIVEN SCADA SYSTEM

For An Enhanced Cybersecurity in a Hospital Management System

Authors

Henry Chima Ukwuoma
Gilles DUSSERRE

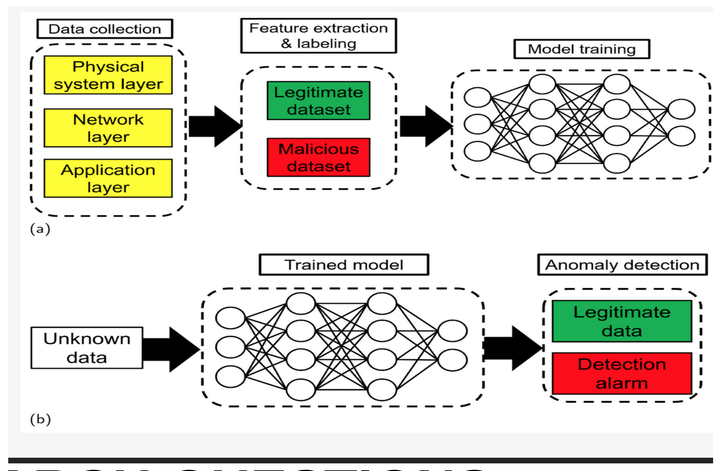
Partners

PTDF Nigeria

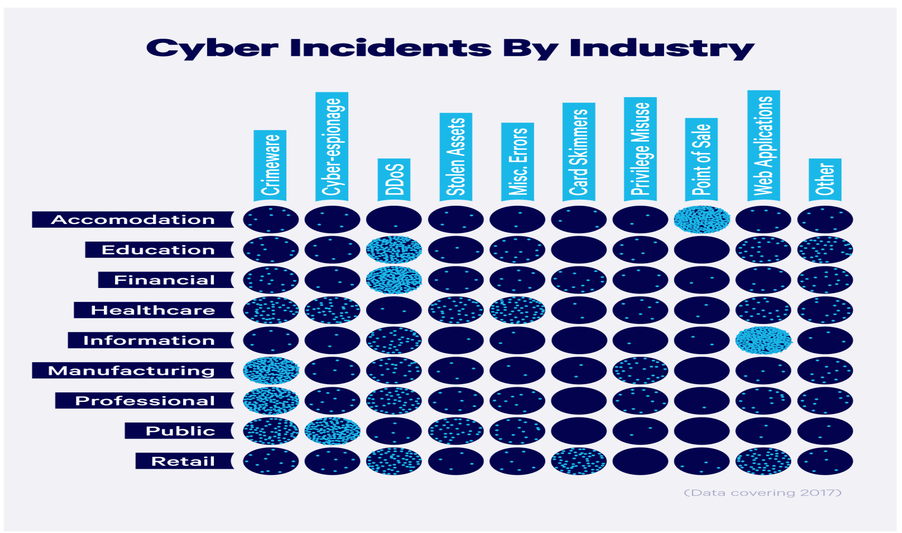
Campus France

BACKGROUND

- **Cyber-Physical system :** A system which comprises of the combination and coordination between computational and physical elements
- **Use of Intrusion Detection Systems:** To alert system administrators and appropriate authorities on unusual access attempts or traffic for an enhanced efficient data management
- **Cybercrime in the Health sector :** With the advent of Covid 19, health facilities have become a target for cyberattacks
- Expectations: Need to prevent and detect access attempts of cyber attacks of any kind in a cyber physical system using computational and physical elements of the system.



Cyber- physical intrusions detections system Source : Kim and Park, 2021



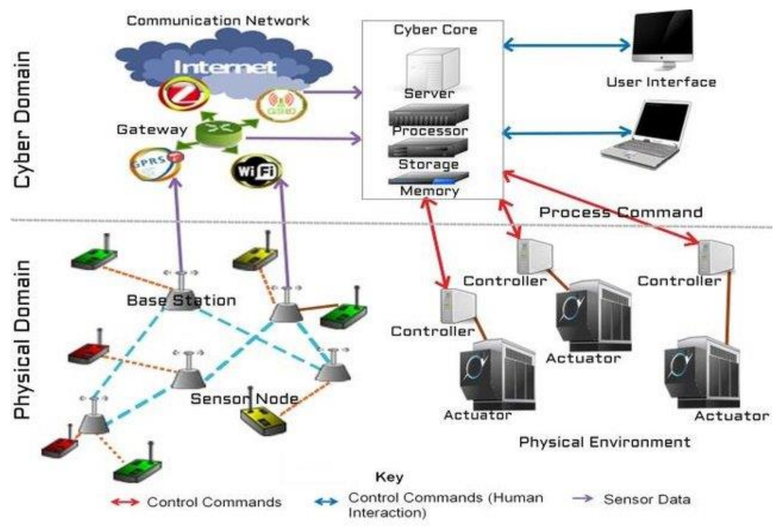
Data Attacks Source :Embroker, 2022

RESEARCH QUESTIONS:

1. **1. How safe are the access control segment of cyber-physical systems**
2. ***2.* What model can be proffered to enhance the access control segment of a cyber-physical system in a hospital environment.**

RESEARCH OBJECTIVES:

- To review relevant literature on the security of cyber-physical systems.
- To design an cyber-physical intrusion detection system for SCADA
- To simulate the proposed system
- To validate the model



Cyber-physical system architecture Source : Ledwaba and Venter, 2017

EXPECTED RESEARCH OUTCOMES:

- A model driven by a post quantum cryptographic algorithm
- A simulation of the proposed algorithm
- Space and time complexity of the proposed algorithm
- Result analysis of the proposed algorithm

References

Kim S, Park K-J. (2021).A Survey on Machine-Learning Based Security Design for Cyber-Physical Systems. *Applied Sciences*. 2021; 11(12):5458. https://doi.org/10.3390/app11125458

Embroker, 2022. 2022 Must-Know Cyber Attack Statistics and Trends https://www.embroker.com/blog/cyber-attack-statistics/

Ledwaba, L. and Venter, H.S. (2017). A Threat-Vulnerability Based Risk Analysis Model for Cyber Physical System Security. Proceedings of the 50th Hawaii International Conference on System Sciences.

Contact : henro317@gmail.com

FEBRUARY 2022 Ecole des Mines D'Ales

Jouer pour mieux gérer une crise, sérieux ?

Une approche ludique et pédagogique

Les multiples enjeux de la formation à la gestion de crise

- **Le constat** est que les dispositifs classiques de formations ne permettent pas une montée en puissance progressive des connaissances et compétences attendus [Fréalle, 2022]
- **L'opportunité** peut résider dans une approche prenant en compte ludicité et mise en pratique de *soft skills* et *hard skills*
- **Une démarche mobilisant le jeu sérieux**, c'est-à-dire tout dispositif dont la finalité première est autre que le simple divertissement [Alvarez, 2007]
- **Notre méthode** est progressive et permet d'explorer la gestion de crise par différentes stratégies ludo-éduquantes

Quelques dispositifs élaborés …

Le Burger Criz

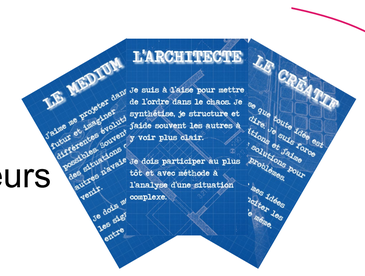
- Quizz
- 60 min
- 6 joueurs
- Mis en œuvre 14 fois
- Objectifs : test des connaissances, prise de décisions intuitives, brise glace

Crisiscape

- Escape game
- 120 min
- 24 joueurs max.
- Mis en œuvre 18 fois
- Objectifs : mise en œuvre de *soft skills*, appréhension des outils d'une cellule de crise et du lieu de simulation

Mission : impossible

- Jeu de cartes
- 20 min
- Sans maximum de joueurs
- Mis en œuvre 7 fois
- Objectifs : brise glace, prise de décisions (créatives versus intuitives), organisation en groupes



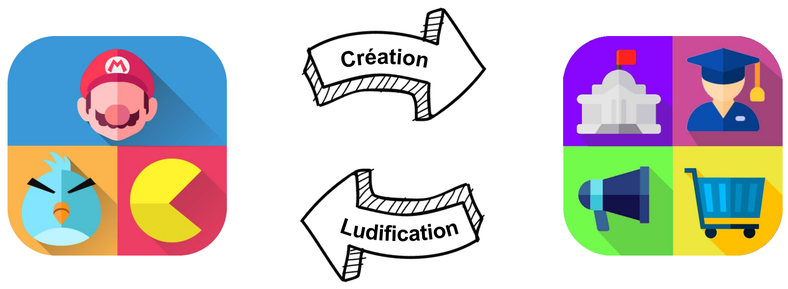
Crise à la carte

- Jeu de cartes
- 120 min
- 8-16 joueurs
- Mis en œuvre 6 fois
- Objectifs : application de connaissances théoriques (aléas, gestion de crise, PCS, acteurs, outils…)

Résultats

Deux approches pour élaborer un jeu sérieux : utiliser des ressorts ludiques pour créer un dispositif nouveau **(création)** ou partir d'un artéfact existant et y ajouter des éléments de *game design* **(ludification)**

Méthodologie fonctionnelle et implantée **depuis 2017** dans les formations à la gestion des risques naturels et technologiques à IMT Mines Alès. Un **continuum pédagogique validé expérimentalement**



Perspectives

- Opportunité d'**étendre la méthodologie** sur la thématique, plus large, de la résilience, intégrant la gestion de crise mais plus largement la gestion du changement ou l'accompagnement à la transition (écologique…)
- Elaboration d'une **méthode d'explicitation des besoins** de parties intéressées
- Démarche guidée pour la conception, l'introduction, la conduite, la remédiation et l'évaluation d'un dispositif ludo-pédagogique

N. Fréalle, P-A. Ayral, E. Piatyszek, *et al.* (2022) Cit'in Crise, a crisis simulator for children adapted from professional training devices. *Article soumis pour publication*

J. Alvarez. (2007). *Du jeu vidéo au serious game : Approches culturelle, pragmatique et formelle*. Thèse de doctorat. Université Toulouse.

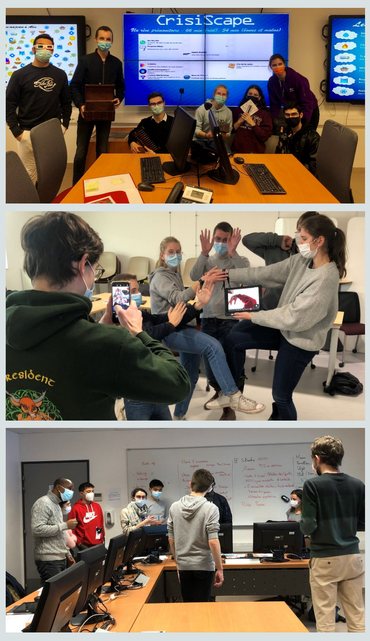
Parties prenantes

IMT Mines Alès
École Mines-Télécom

Auteurs

Florian Tena-Chollet
Noémie Fréalle

Palmarès



Clins d'œil

> Au dispositif **Cit'in Crise**, autre jeu sérieux développé avec Mines Saint-Etienne, la Rotonde et les Petits Débrouillards

> A l'Unité d'Enseignement « **Résilience : enjeux en jeu** » à IMT Mines Alès

Remerciements

Philippe Bouillet
Elise Carton
Maxence Corailler
Dimitri Lapierre
David Martin

Et à Alain Chabat pour son aimable autorisation à adapter le concept du Burger Quiz

Contact : florian.tena-chollet@mines-ales.fr

Colloque Gestion de Crise et Numérique – IMT – Palaiseau (91) Mars 2022

Simulations de gestion de crise
2 outils et 12 années d'expérience
aux Mines Saint-Etienne

pour un public opérationnel, étudiant et citoyen

Objectif : Sensibiliser les participants à la complexité de la gestion de crise.


L'EST RÉPUBLICAIN

ENSEIGNEMENT

Gestion de crise aux Mines

L'école d'ingénieurs vient de mettre au point un outil extraordinaire de simulation. Exercice concluant, jeudi…

Le simulateur de gestion de crise est censé surprendre les professionnels de la gestion de crise dans leur manière de travailler… Photo Dominique CHARTON

Le projet est d'une telle importance que des observateurs parisiens de la sécurité civile ont fait le déplacement, jeudi, à l'École des Mines de Nancy, pour se rendre compte de la manière dont fonctionne l'outil mis au point, depuis deux ans et demie, en collaboration avec une dizaine de laboratoires des campus nancéiens.

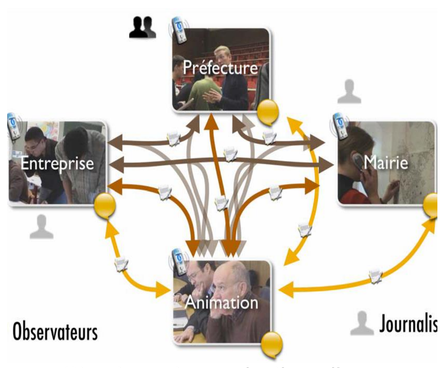
Il s'agit d'un système créé pour simuler des gestions de crise, d'un outil de communication à destination des acteurs ayant un rôle à… cia Tardy, coordinatrice du projet, Jack-Pierre Piguet, directeur de l'École des Mines, et Thierry Verdel, responsable et initiateur du projet. Lestrois cellules actives étaient quant à elles constituées de vrais professionnels de la préfecture de Meurthe-et-Moselle, de la mairie de Jœuf, dont le maire en personne, de pompiers, de techniciens.

L'outil imaginé par les enseignants chercheurs nancéiens ressemble à un forum de discussions sur internet. A la différence qu'il permet décrire, *les informations transmises. C'est pour ça que notre outil est spécifique. Car il est pluridisciplinaire. Faisons intervenir les sciences techniques aussi bien que les sciences humaines».*

Sous les eaux…

Jeudi, il s'agissait de noyer sous les eaux la commune de Jœuf. De voir comment les secours étaient déclenchés. D'ajouter quelques incidents comme de grands glissements de terrains, une paralysie des voies de

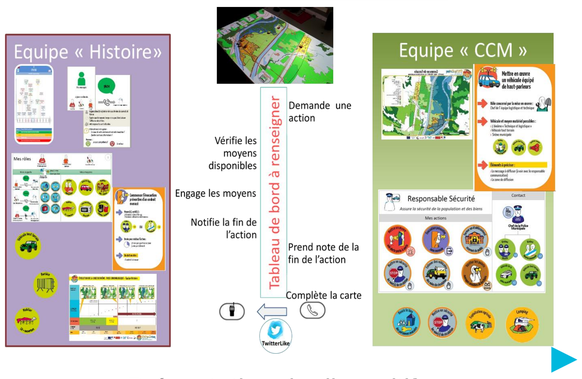
Article de Philippe Mercie paru le 6 novembre 2009



Structure et organisation d'une simulation classique iCrisis

En dessous : la cellule d'animation pendant la crise sanitaire, en mode hybride, connectée à iCrisis

Exemples de simulation



Présentation du dispositif

Nuage de mots – retour des joueurs

- **Pour les étudiants de niveau master/ ICM** – Apporter des compétences complémentaires à leur formation dans l'esprit de la prévention et la sensibilisation aux risques majeurs;
- **Pour des acteurs professionnels** – Développer leurs capacités de prise de décision dans un contexte complexe et incertain, expérimenter les nouveaux scénarii impliquant les partenaires opérationnels territoriaux, valider existant;
- **Pour le grand public** – Sensibiliser et former d'une manière ludique pour qu'il devient un acteur conscient et rationnel facilitant la gestion de crise réelle;
- **Pour les élus communaux** – Faire découvrir l'univers de la cellule de crise (organisation, objectifs…) et la nécessité d'une réflexion préventive approfondie pour la mise en place d'un Plan Communal de Sauvegarde opérationnel.

iCRISIS™

- **Genèse –** Né à la fin des années 2000 au laboratoire LAEGO (Mines de Nancy), développé ensuite entre 2008 et 2010 (RD&T 2006), en collaboration notamment avec les Mines Saint-Étienne, a fait objet d'une thèse soutenue en 2019 (C.Judek);
- **Dispositif** – technique et organisationnel, doté d'un logiciel internet-based; autoévaluation par les participants de leurs capacités à la prise de décision dans une situation complexe d'une crise.
- **Méthode** – plusieurs cellules de crise distantes communiquent entre elles et avec une cellule d'animation composée d'opérationnels et de chercheurs; L'ensemble des échanges est mémorisé dans le système et analysé pendant un débriefing à chaud. La scénarisation est « légère » et flexible, adaptable, sans la programmation lourde;
- **Utilisation** – depuis 2009, pour la formation des ICM et des Masters (Saint-Étienne, Nancy, Paris, Lyon, IRA Metz; aussi à distance - env. 8 simulation/an depuis 2020).
  - Pour des opérationnels de services d'Etat et collectivités territoriales lors de simulations spécifiques nationales (Restoterin Bordeaux, Direction de l'Université et Métropole de Loraine, etc.) et internationales (Université de Senghor – Alexandrie)
  - Comme outil d'évaluation de dispositifs existants dans le cadre de 3 projets internationaux de recherche ; au total prés de 80 simulations réalisées.

CIT'IN CRISE

- **Genèse :** Né à la fin 2019, et développé par Mines de Saint-Etienne et IMT Mines Alès dans le cadre d'un appel à projet du Plan Rhône. Conçu à partir de l'expérience des 2 simulateurs ICRISIS ™ et Simulcrise (Mines Alès)

- **Dispositif** Un dispositif type serious game utilisant plateaux de jeu, jetons, cartes à jouer, talkiewalkies, téléphones, tablettes permettant de vulgariser un plan communal de sauvegarde afin de plonger le grand public et/ou des élus dans l'univers de la gestion de crise communale.
- **Utilisation** Employé lors d'une centaine de simulations avec du grand public, des scolaires (cycle 3) et des élus communaux.

Contact : tardy@emse.fr, piatyszek@emse.fr

Auteurs

Alicja Tardy
Eric Piatyszek

Partenaires

Financeurs

31 Mars 2022 Colloque de l'Institut Mines Télécom

Management of citizen & volunteers:

Social media in crisis situation

Résumé :

MACIV étudie les flux d'information et les initiatives citoyennes sur les media sociaux lors d'un évènement majeur afin d'accompagner les acteurs de la gestion de crise à les intégrer dans leurs pratiques. Il vise également le développement d'un module dédié à la gestion des volontaires au sein de la plateforme RIO-Suite.

Parties prenantes

Auteurs

Robin Batard
Frederick Benaben
Sandine Bubendorff
Florent Castagnino
Julien Coche
Aurélie Montarnal
Valérie November
Caroline Rizza (leader)

Partenaires

CONTEXTE

MACIV a été défini sur 2 ans

1. Contexte français :

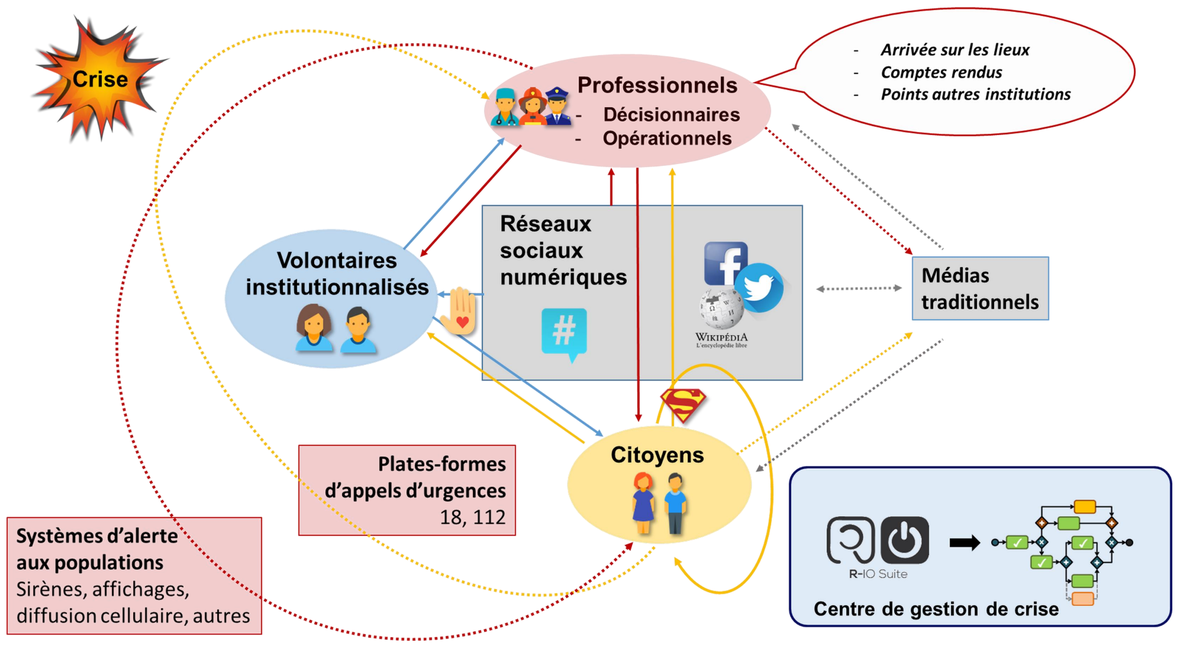
Les crues (Loiret et Var 2015) et les attentats (Paris 2015 et Nice 2016) et l'émergence de l'utilisation des media sociaux) par les citoyens (*FB safety check*, *#parisportesouvertes*).

2. Contexte scientifique :

Des recherches ancrées dans les pratiques professionnelles :

- Le consortium Euridice (LATTS, Préfecture)
- La plateforme RIO-Suite (IMT-Mines Albi)
- La communauté internationale ISCRAM
- Des rapports privilégiés avec les partenaires institutionnels (VISOV, SDIS, DG)

VUE GENERALE DE L'OBJET D'ETUDE



OBJECTIFS

Objectif 1 : Etudier la réorganisation des circuits d'information entre les citoyens/volontaires, les opérationnels et les gestionnaires de crise

- Intégrer volontaires et citoyens dans les processus de gestion et de réponse à la crise
- Aider à l'adaptation des pratiques professionnelles
- Améliorer la résilience des populations affectées.

Objectif 2 : Développer un module "media sociaux et citoyens " au sein de la plateforme RIO-Suite dédié à la collecte de données afin de les traduire en information pertinente pour les utilisateurs finaux

- Gérer des flux d'information en amont et en aval
- Intégrer les outils préexistants des professionnels
- Intégrer les techniques émergentes basées sur le web.

MÉTHODOLOGIE

Documenter les réactions citoyennes sur les media sociaux

1. Media sociaux, gestion de crise et volontaires
   - Etude bibliographique
   - Observation des VISOV et des pratiques institutionnelles (media sociaux/veille)
2. Définition d'un "espace de conception" et d'une "taxonomie des tâches"
   - Les outils, systèmes et plateformes utilisés par les citoyens et leurs objectifs pendant la crise
3. Des études de cas pour documenter l'utilisation des RSN pendant une crise
   - La manière dont les citoyens sont engagés dans la gestion et la réponse,
   - Les conséquences inattendues associées

RÉSULTATS

1. **Une meilleure compréhension des pratiques des acteurs (gestionnaires, SDIS, VISOV et citoyens)**
   - Rapports sur les pratiques des acteurs et la circulation de l'information lors d'une crise
   - Thèse sur l'intégration des initiatives citoyennes en gestion de crise (Batard, 2021)
   - 3 exercices SDIS, COD, COZ et RETEX auprès des professionnels
2. **La plate-forme de médiation et les outils associés**

Thèse sur le développement d'un outil de traitement des media sociaux à destination des gestionnaires de crise (Coche, 2022)

Contact : caroline.rizza@telecom-paris.fr

Sécurité des objets connectés

Analyse de la sécurité des systèmes embarqués

Automatisation des techniques de tests Hardware-in-the-loop

Parties prenantes

Auteurs

Paul OLIVIER
Aurélien FRANCILLON

Partenaires

Motivations

- Les systèmes embarqués sont constitués d'une grande variété de composants, ce qui en fait des **systèmes complexes**.
- Le manque de connaissance de leurs composants internes et le peu de contrôle sur leur exécution conduisent à les considérer comme des **boîtes noires**.
- L'émulation est un outil puissant mais demeure limitée par un support hétérogène inhérent à la diversité des composants matériels.
- **L'exécution logicielle hybride** permet d'exécuter le code dans un émulateur générique alors que les interactions matériels sont transmises au dispositif physique.

Avatar²: le chef d'orchestre [1]

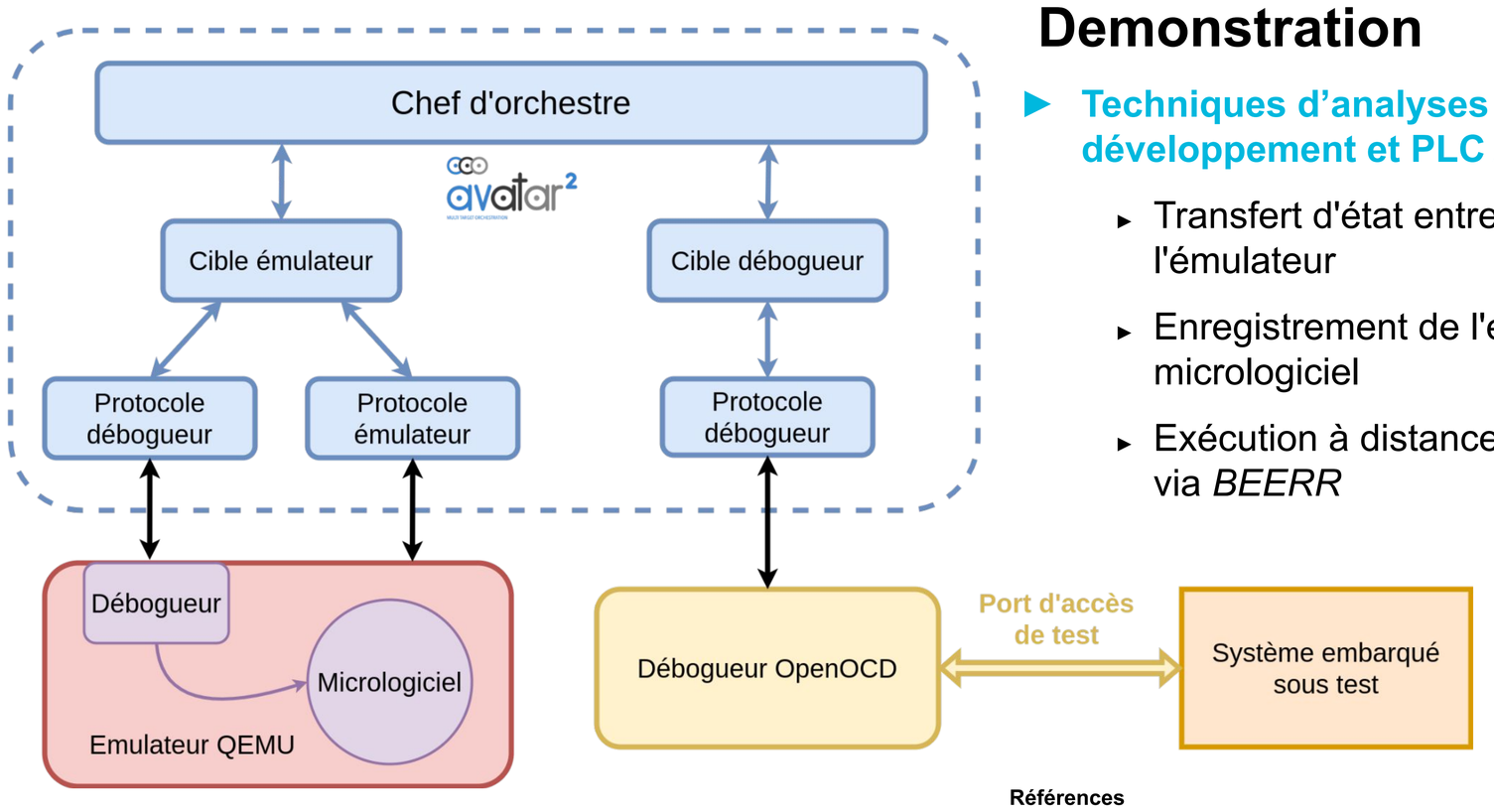
- ***Comment combiner plusieurs outils d'analyses binaires pour étudier des systèmes embarqués ?***
- Améliore **l'interopérabilité** entre plusieurs outils d'analyses dynamiques binaires (débogueur, émulateur, exécution symbolique):
  - **Orchestre** les différentes cibles / outils.
  - **Transfert l'etat** et **synchronise** le matériel avec l'émulateur.
  - Transfert les **accès mémoires** au matériel.
- Offre la possibilité de connecter des systèmes physiques dans un émulateur à l'aide d'un débogueur (Hardware-in-the-loop).

BEERR: Banc d'expérimentations sur des systèmes embarqués pour une recherche reproductible

- ***Comment améliorer la reproductibilité des expérimentations de sécurités sur les systèmes embarqués ?***
- Un environnement pour mieux étudier les expérimentations sur la sécurité des systèmes embarqués:
  - Rassemble une **collection d'expérimentations** prête à être utilisée.
  - **Automatise la mise en place** des expérimentations.
  - Facilite l'accès aux dispositifs physiques **à distance**.

Demonstration

- **Techniques d'analyses sur une carte de développement et PLC Allen Bradley [2]**
  - Transfert d'état entre le matériel et l'émulateur
  - Enregistrement de l'exécution du micrologiciel
  - Exécution à distance de l'expérimentation via *BEERR*



Contacts: {paul.olivier, aurelien.francillon}@eurecom.fr

Références

[1] M. Muench, D. Nisi, A. Francillon, D. Balzarotti, "Avatar2: A multi-target orchestration platform", BAR 2018.

[2] L. Garcia, F. Brasser, M. H. Cintuglu, A.-R. Sadeghi, O. Mohammed, and S. A. Zonouz, "Hey, my malware knows physics attacking PLCs with physical model aware rootkit", NDSS 2017.

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

CHAIRE CYBER CNI
Sécurité des infrastructures critiques

cyber-cni.fr/

PhD Thesis

Federated Approaches for Defending Cyber-Attacks

Author

Léo LAVAUR

Advisors

Marc-Oliver PAHL
Yann BUSNEL
Fabien AUTREL

School

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Partners

AIRBUS DEFENCE & SPACE

BNP PARIBAS
La banque d'un monde qui change

EDF

NOKIA Bell Labs

SNCF

CHAIR OF CYBER CNI
Critical National Infrastructures

I. Context and Aims

- In 2016, Google introduced the concept of **Federated Learning (FL)**, enabling collaborative Machine Learning (ML). FL does not share local data but ML models, offering applications in diverse domains. FL has been studied to overcome challenges of **collaborative intrusion detection** and mitigation systems, such as communication overhead and information disclosure.
- This thesis addresses current limitations of Federated-learning Intrusion Detection and mitigation Systems (FIDS) in terms of **transferability, adaptability and scalability**. The chair's realistic test beds [1] will be used to host experiments and validate our hypotheses. The long-term objective is to build a distributed collaborative observatory of cyber-threats that would feed the detection systems of organizations.
- While our work on the literature answered multiple questions already, the following research questions are open:

  RQ1: What are the relevant features to train FIDSs?

  RQ2: How can we federated knowledge between parties with different use cases?

  RQ3: Is there a trade-off between model specialization and generalization for FIDSs?

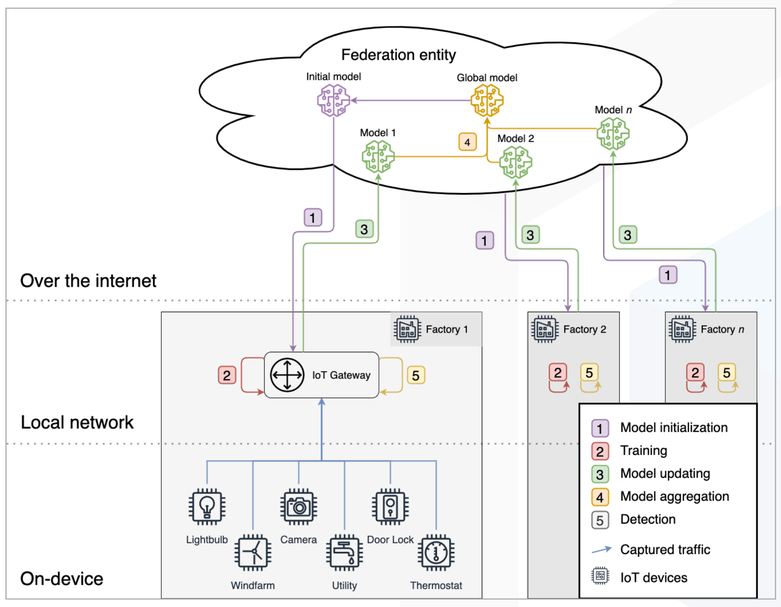


Fig 1: Federated Learning for intrusion detection in Industry 4.0 [2]

II. State of the Art of FIDSs

- We focus on FL-based intrusion detection systems (or FIDSs), which has become the state of the art for Collaborative IDSs (CIDSs). A survey paper [2] has been submitted to TNSM in 2021 and is currently under review. In particular, this **Systematic Literature Review (SLR)** shows: (a) how FIDSs are used in different domains; (b) what differences exist between architectures; (c) the state of the art of FIDSs.
- FIDSs are a *trending topic* whose evolution is following the one of FL. Publications are heterogeneous in term of venues and research groups. Most publications are use-case–based.

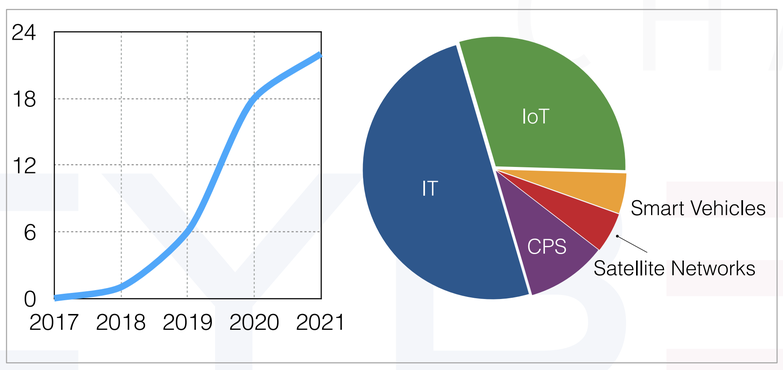


Fig 2: Evolution and repartition of FIDSs publications [2]

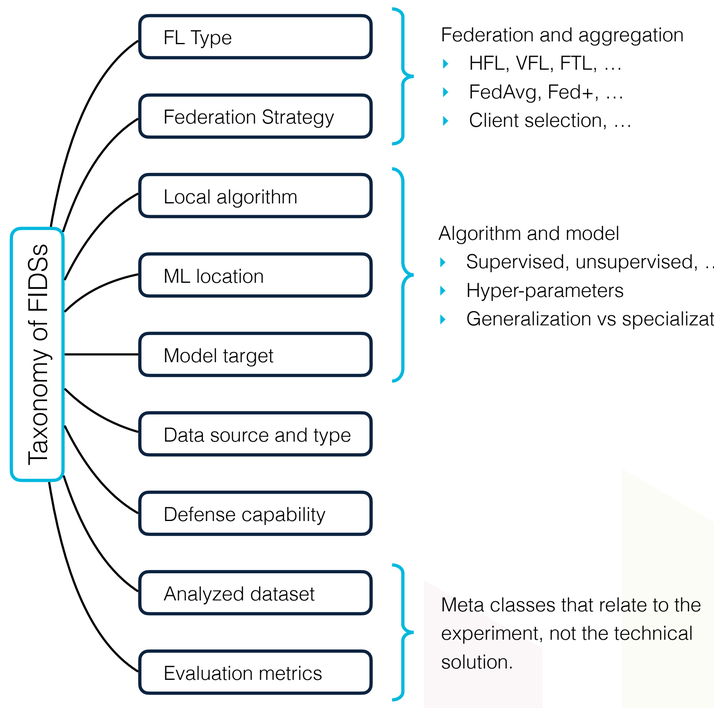


Fig 3. Taxonomy of FIDSs [2]

- The survey highlighted research directions for the community to follow. FIDSs have limited adaptability when dealing with architectures that are too different. Therefore, we will first work on **knowledge transfer in heterogeneous federations**: heterogeneous data, models, or features are considered.
- Other relevant research directions include **adaptability**—eg. dealing with data changes or clients with different distributions—, and **scalability**—eg. high number of clients, hierarchical federation aspects.
- The community identified other open issues, mostly **performance**– and **security**-wise.

III. Future work

- The chair builds and hosts realistic test beds to perform real-life reproducible experiments. Three use cases are considered in this thesis: IT infrastructures, industry 4.0, and smart buildings. The three use cases are covered by the chair's test beds and its partners. Two projects will start to address FIDSs limitation:

  P1: FIDS-EP: an evaluation platform for reproducible experiments

  P2: Cross-Silo and Hierarchical FL for FIDSs

IT networks | Industry 4.0 | Smart buildings

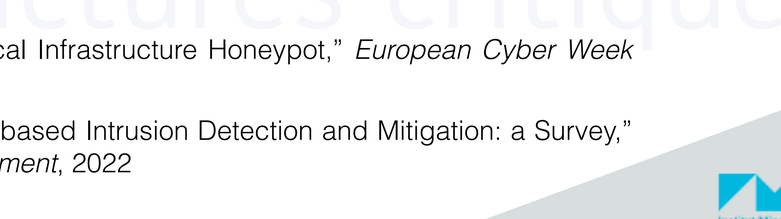


Fig 4: Test beds of the chair Cyber CNI: Airbus Cyberrange, Fischertechnics models, Cencyble building (Rennes campus)

- One of the major caveats of the literature review is the i**nability to compare the performance of existing approach**, due to the differences in term of dataset, algorithms, participants, and use case. Therefore, we will develop an **evaluation platform for reproducible experiments**. This will allow us to study the impact of existing FL strategies on performance, and eventually provide objective insights on FIDSs design.
- The second project addresses the transferability and adaptability aspects of FIDSs to match the needs of organisations. Cross-silo FL enables privacy-preserving **training of heterogeneous models**, so that each organization can train a model of its own, while benefiting of the experience of the other participants. This is extremely relevant for IDS tasks. Organisation could train a model locally with FL among agents, and collaborate externally, using a **hierarchical approach**.

References

[1] M.-O. Pahl, A. Kabil, E. Bourget, M. Gay, and P.-e. Brun, "A Mixed-Interaction Critical Infrastructure Honeypot," *European Cyber Week C&ESAR Conference*, 2020.

[2] L. Lavaur, M.-O. Pahl, Y. Busnel, and F. Autrel, "The Evolution of Federated Learning-based Intrusion Detection and Mitigation: a Survey," under review *in IEEE TNSM Special Issue on Advances in Network Security Management*, 2022

Contact: leo.lavaur@imt-atlantique.fr
Twitter: @phdcybersec
Github: @phdcybersec
LinkedIn: linkedin.com/in/leo-lavaur

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

CHAIRE CYBER CNI
Sécurité des infrastructures critiques

cyber-cni.fr/

Phd thesis:

Automated learning and handling cyber-physical attacks.

Awaleh HOUSSEIN MERANEH

Author:

Advisors:

Marc-Oliver Pahl
Hélène Le Bouder

School:

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Partners:

AIRBUS

AMOSSYS

eDF

NOKIA Bell Labs

BNP PARIBAS
La banque d'un monde qui change

CHAIRE CYBER CNI
Critical National Infrastructures

1-) Thesis context

Cyber-physical systems (CPSs) integrate the physical and cyber worlds via a communication network. This integration makes the CPSs vulnerable to certain type of cyber-physical attacks (e.g., Stuxnet). A focused application of CPSs is in industrial control systems (ICS) which is the interest application of this research.

The primary objective of this thesis is to propose an approach to detect cyber-physical attacks against ICS. Establishing an anomaly detection approach is important for the regular monitoring of the system's behavior.

Indeed, anomaly and intrusion detection for ICS is a widely studied subject in the literature. Intrusion Detection Systems (IDS) commonly used method of intrusion and anomaly detection in ICS. Many types of IDS are proposed, such as signature-based, specification-based and behavior-based.

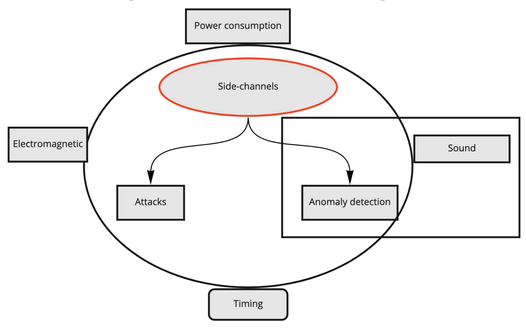
We firstly investigate the behavior-based type of anomaly detection. Side-channels is used to represent the normal and abnormal behavior of the systems.

RQ1: How can side-channels used to detect abnormal behavior of the ICSs?
- **RQ1-1:** How to detect anomalies by using sound-based anomaly detection ?

2-) State-of-the-art

2-1) Background of side-channels

- Side-channel is often used to attack (retrieve secret data) of a cryptographic algorithms.
- Recently, the side-channels is applied to detect abnormal behavior in ICS.
- Side-channels use a variety of physical leakage parameter to attack or to detect, such as electromagnetic, sound, timing and so on.

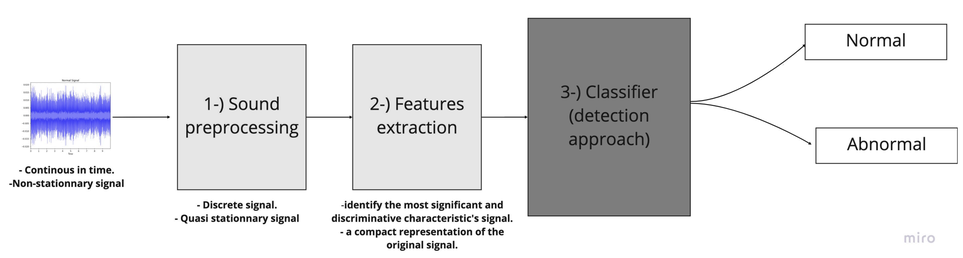


Overview of side-channels
Source: Awaleh Houssein

- In a first time, we focus on side-channel based anomaly detection of ICS using sound as leakage parameter.

2-1) Overview of Sound-based Anomaly Detection (SAD)

- Sound-based anomaly detection (SAD) is the task of detecting whether a target machine sound is normal or abnormal.
- SAD is a research field used for a variety of application domain such as public surveillance, speech analysis, healthcare, predictive maintenance and cyber-attack detection.



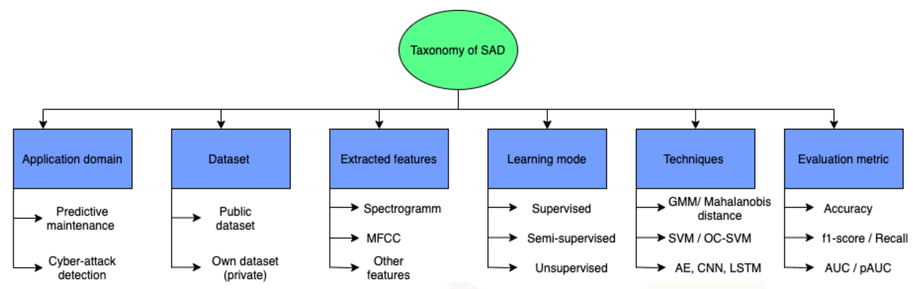
SAD overview
Source: Awaleh Houssein

- In ICS, predictive maintenance application is used to detect systems failure, whereas cyber-attack detection application is used to detect cyber attacks.

3-) Current work

3-1) Survey of sound-based anomaly detection of ICS

- The research question addressed in this paper is how to detect both systems failures and cyber-attack using sound.
- The reviewed studies of the survey are classified and presented according to the following taxonomy:



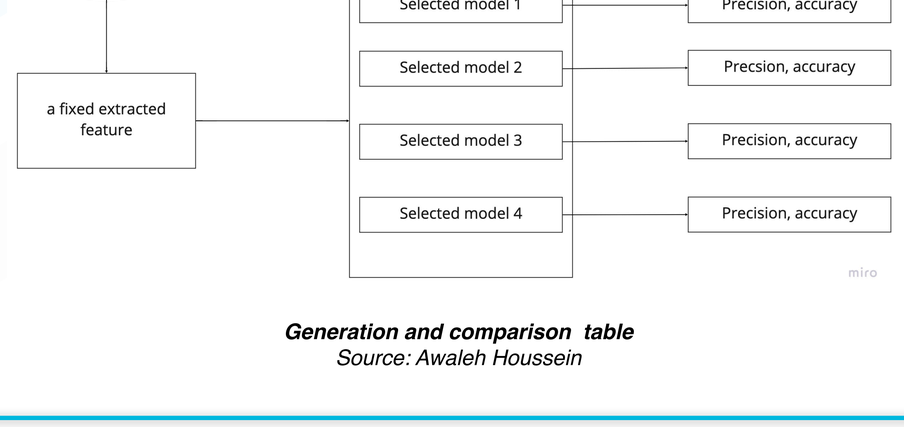
Taxonomy of SAD
Source: Awaleh Houssein

3-2) Comparison of some reviewed techniques

Following the review of the ICS sound anomaly detection papers, it was noted that the techniques use a variety of datasets and extracted features to validate their approaches.

This is why comparing some of the reviewed studies by using the same dataset and a fixed extracted feature seemed us relevant.

Our sound dataset are generated using a Fishertechnick model that represents a muniatarized industrial system. This model is composed of the following subsystems: a conveyor, a pneumatic system, a robot arm, and an indexed line.



Generation and comparison table
Source: Awaleh Houssein

4-) Planned work

- Propose an appraoch of SAD detecting both system failure and cyber-attacks.
- Adding another leakage parameter (e.g electromagnetic) to stronger our proposed approach.

Contact: awaleh.houssein-meraneh@imt-atlantique.fr

This poster was made at the chaire Cybersecurity for Critical Networked Infrastructures (Cyber CNI) | https://cyber-cni.fr/ | Our monthly cybersecurity speaker series https://talk.cybercni.fr/ | Our science blog https://future-iot.org/

Machine Learning and Data Visualization for CyberAttacks Detection

Auteurs

Robin Duraz

Partenaires

ECOLE NAVALE

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

ENSTA BRETAGNE

NAVAL GROUP

THALES

PÔLE D'EXCELLENCE CYBER

Région BRETAGNE

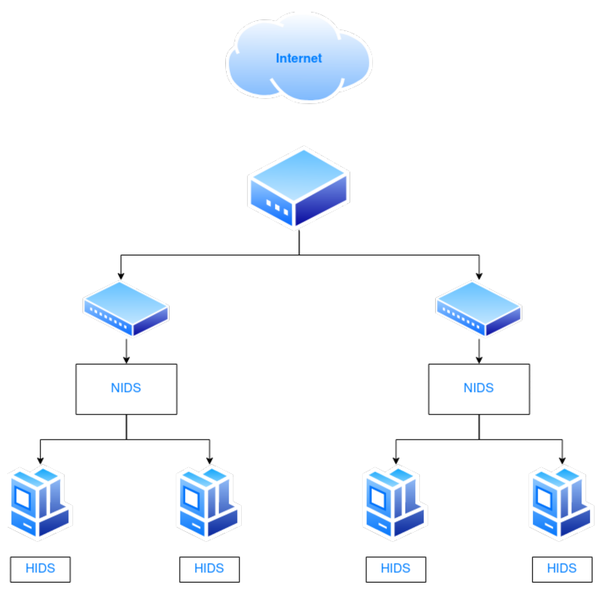
Problem

Technology pervades our world with all sorts of connected devices, be it in our professional or personal environments. Along with that comes new threats, forcing domain experts to devise **new security measures**.

Machine Learning can help create **Intrusion Detection Systems (IDS)** that can hopefully :

- Adapt to changing threats
- Keep working with trafic that is more and more encrypted

But what kind of performance can we expect from Machine Learning algorithms ?



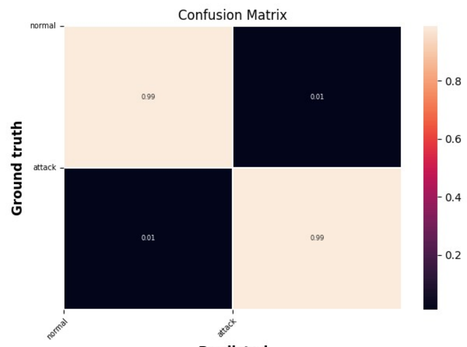
CICIDS 2017

A dataset with a quite complete environment, with simulated normal trafic and 14 different attacks performed.

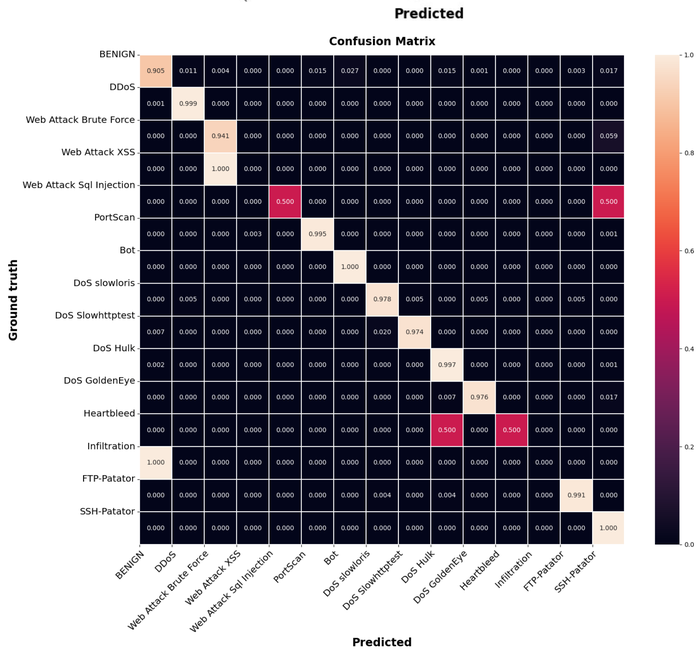
Sharafadin et al., 2018

Botnet (Ares)	**Remote shell, keylogging and others**
DDoS	**Junk TCP, UDP and HTTP GET requests**
DoS GoldenEye	**Uses HTTP KeepAlive and NoCache**
DoS Hulk	**Dynamic requests**
DoS Slowloris DoS Slowhttptest	**Keep connection open by continuously sending small packets**
FTP/SSH-Patator	**Brute force attack over FTP/SSH**
Heartbleed	**Attack on a vulnerable SSL version**
Infiltration	**Uses an infected dropbox file or USB key to perform a portscan attack**
Portscan	**Nmap with various options, sS, sT, sF, etc.**
Web Attack Brute Force / SQL Injection / XSS	**Performed on a vulnerable PHP/MySQL Web App**

Performance



Performance obtained by a neural network seems almost perfect when trying to differentiate normal trafic from attacks, even with really simple networks.

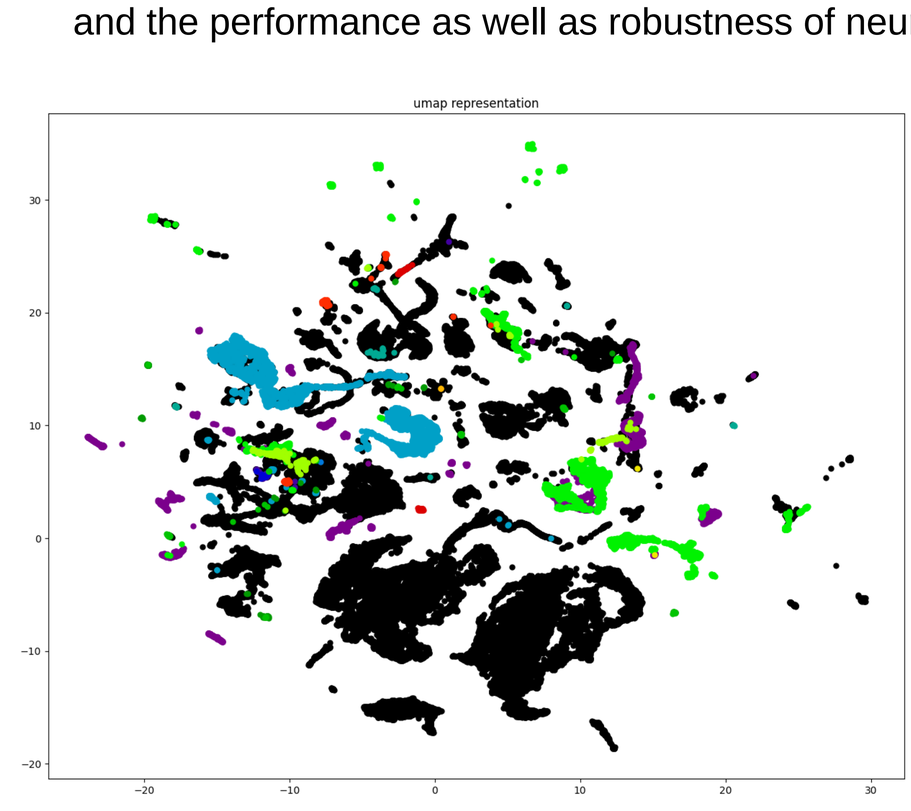


But they aren't so perfect if we consider attacks separately, even for better networks.

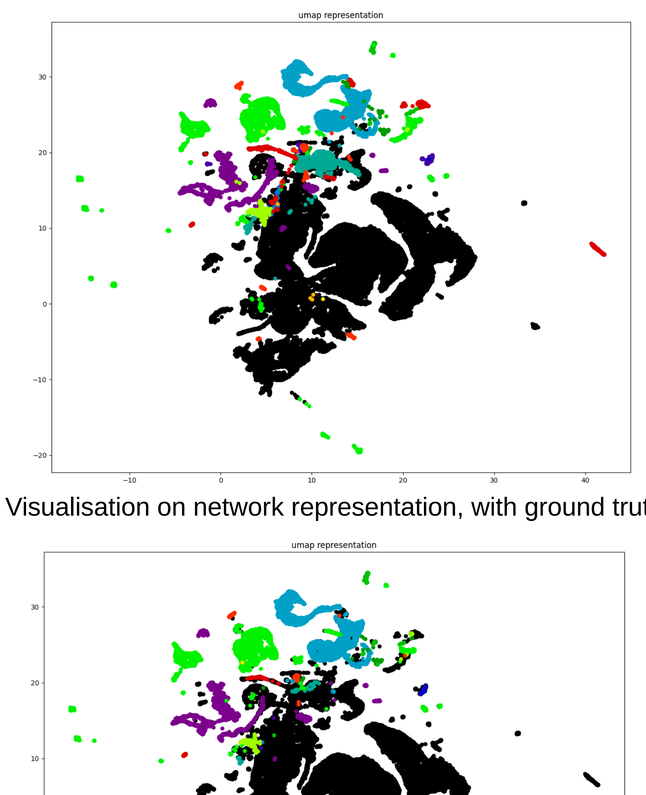
One attack is completely missed, and a few are largely missclassified.

Visualization to explore data and network representations

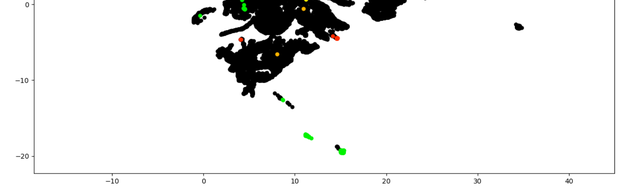
Visualization tools can help estimate the complexity of the task, and the performance as well as robustness of neural networks.



Visualisation on original data



Visualisation on network representation, with ground truth



Visualisation on network representation, with network predictions

Contact : robin.duraz@imt-atlantique.fr

SCABox un outil pour étudier les attaques matérielles à distance

Institut Mines-Télécom

Parties prenantes

MINES Saint-Étienne

Une école de l'IMT

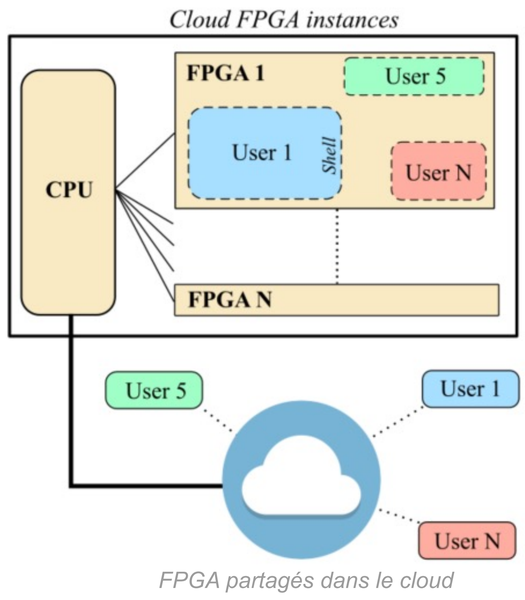
Institut Mines-Télécom

Auteurs

Joseph Gravellier
Jean-Max Dutertre
Sami Dahoux
Yannick Teglia
Philippe Loubet Moundi

Partenaires

THALES

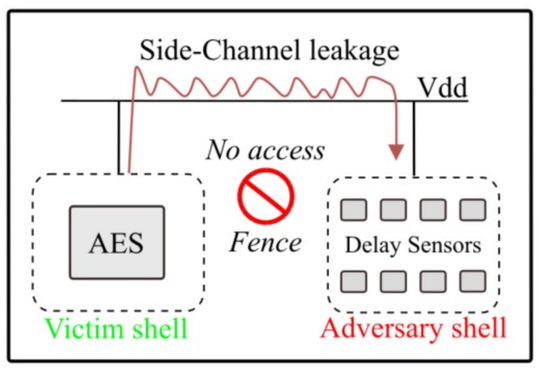


FPGA partagés dans le cloud

Contexte

Adoption des FPGAs dans le cloud

- **FPGA dans le cloud** – Les grands fournisseurs de cloud ont récemment déployés des FPGA dans leurs serveurs (Amazon EC2, Alibaba F3, etc).
- **Ressources partagées**– La logique FPGA peut-être louée et partagée entre plusieurs utilisateurs. Chaque locataire est confiné dans sa logique dédiée à l'instar d'une machine virtuelle
- **Problème** – Les FPGAs multi-utilisateurs pourraient être pris pour cible par des attaques matérielles à distance

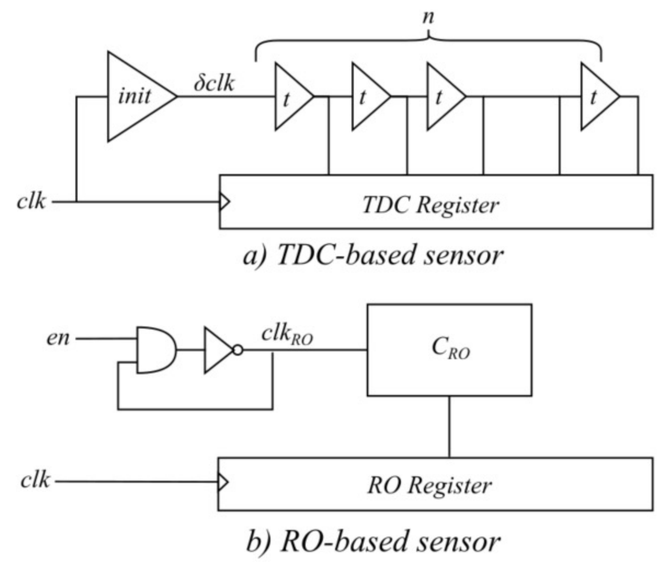


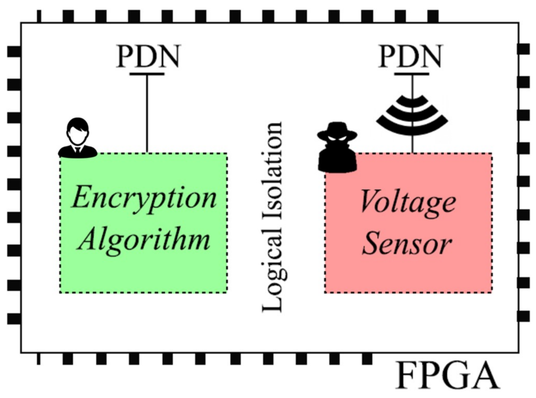
Modèle de menace

- Un utilisateur **victime** utilise l'accélération FPGA pour effectuer des chiffrements ou des calculs de réseaux de neurones.
- Un utilisateur **attaquant** implémente des capteurs de tension dans le FPGA pour espionner l'activité de la victime.

Capteurs de tension intégrés

- Les capteurs de tension convertissent les variations de consommation électrique induites par l'activité de la victime en information digitales.
- Les capteurs principalement utilisés sont le *Time-to-Digital Converter* (a) et *le ring-oscillator* (b).



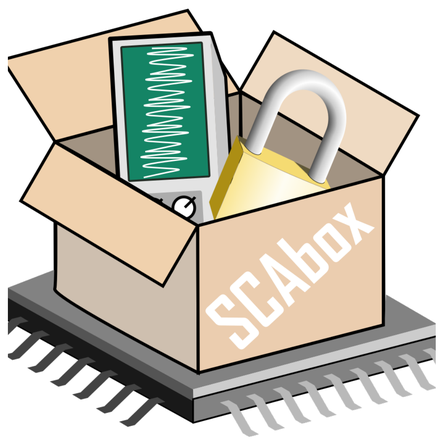


Extraction de secrets cryptographiques

- L'écoute de la consommation d'un algorithme de chiffrement permet **l'extraction de sa clé à distance** !
- L'isolation entre la **victime** et **l'attaquant** est compromise

Projet SCABox

Un outil pour réaliser des attaques par canaux-cachés sur FPGA



Logo SCABox

- **À but éducatif** – Familiarisation avec les attaques par canaux-cachés
- **À but sécuritaire** – Outil d'évaluation de la fuite électrique d'algorithmes de chiffrements
- **Destinataires** – étudiants et évaluateurs de sécurité matérielle
- Disponible sur GitHub avec un tutoriel complet: https://github.com/emse-sas-lab/SCAbox
- Addition prévue de nouveaux capteurs et de nouveaux algorithmes dans le futur

Contact : dutertre@emse.fr

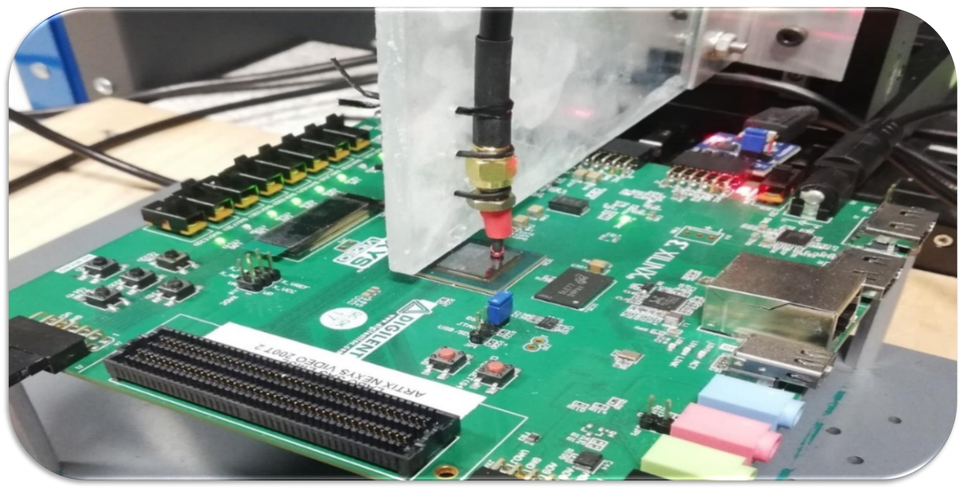
Mars 2022 Colloque de l'Institut Mines Télécom Paris

Securing The IoT Against Fault Injection Attacks Using Digital Sensors

Advanced **PR**ivacy of **IO**t devices through **R**obust Hardware **I**mplementation (APRIORI)

➢ **Problematic:** The **I**nternet **O**f **T**hings *(IoT)* is about networking physical objects through the Internet. The confidentiality and security of sensitive data (passwords) exchanged between IoT devices are potentially at risk of being broken by attackers using fault injection attacks.

➢ **Objective**: Design a fully digital sensor against fault injection attacks.



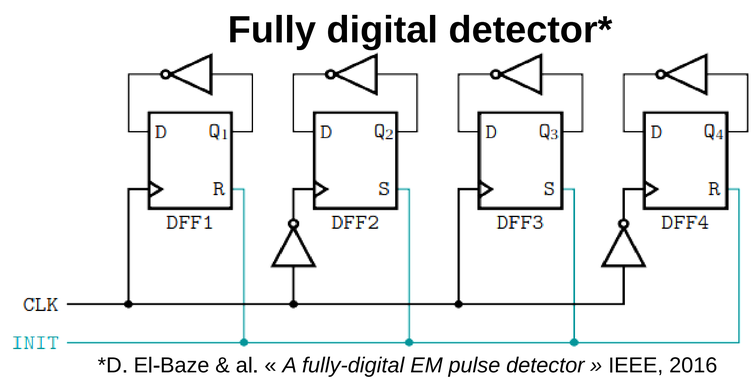
➢ Extract confidential data from an **I**ntegrated **C**ircuit *(IC)* by means of **E**lectro**M**agnetic **F**ault **I**njection *(EMFI).*

➢ Generate an EM perturbation near the circuit *(voltage transient through a home-made EM probe*).

➢ Target:
Nexys video 7 board (*Xilinx Artix7-200T).*
AES128 + 16 sensors.

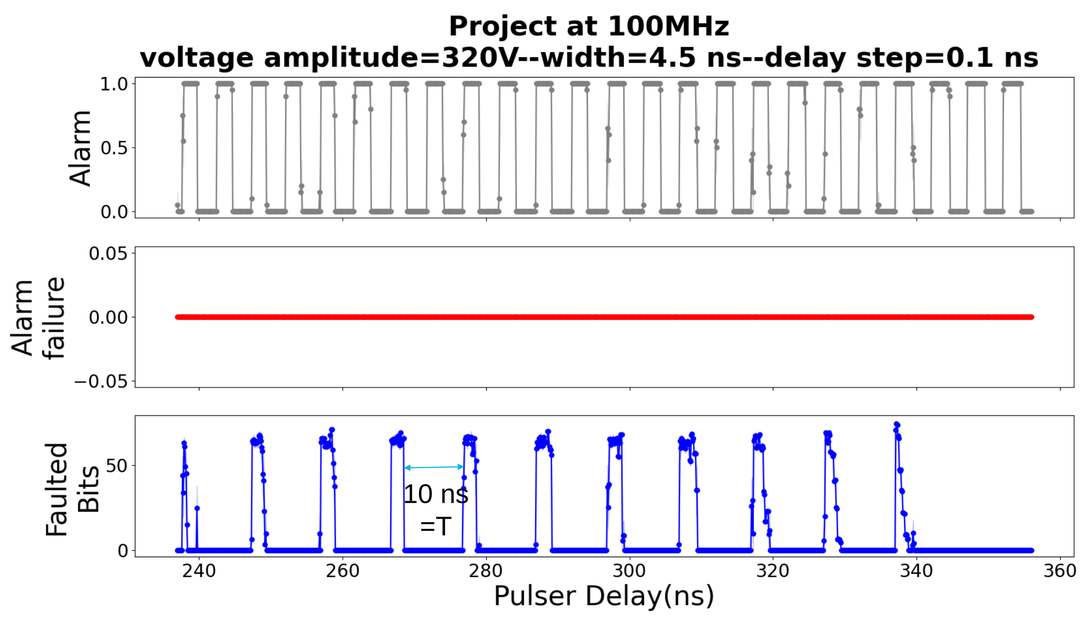
➢ Programmable clock frequency:
MMCM from 10 to 200 MHz.

Fully digital detector*



*D. El-Baze & al. « *A fully-digital EM pulse detector* » IEEE, 2016

➢ Study the effectiveness of the fully digital detector* against EMFI.
➢ Examine the triggering of the detectors and the number of faulted bits at different frequencies from 100 MHz to 200MHz.

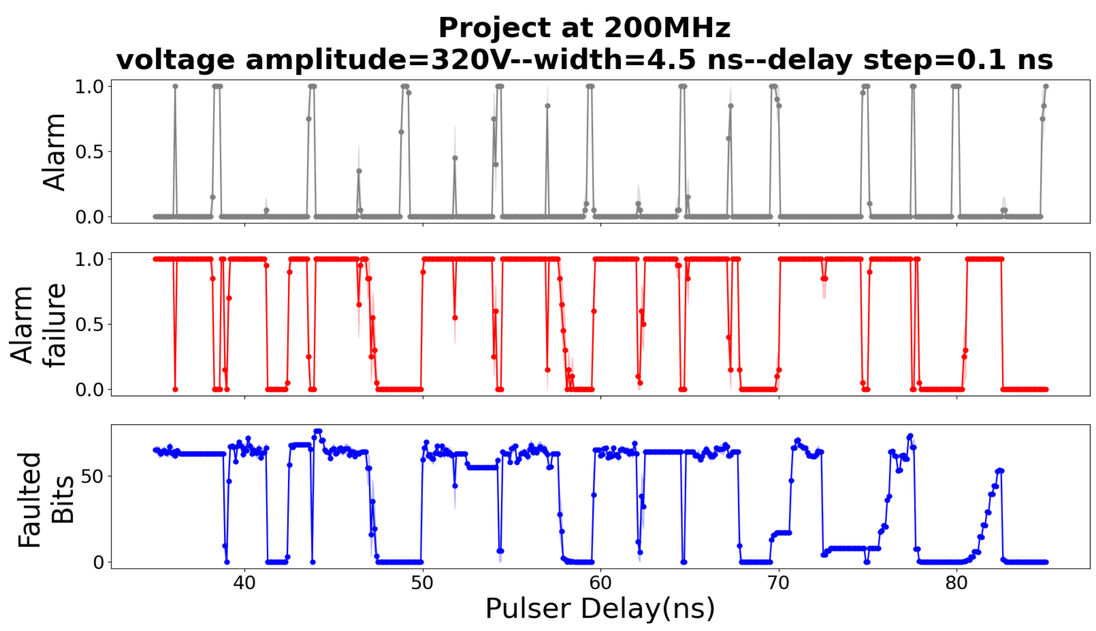


➢ At 100 MHz:

- Detect all injected faults.
- Injected faults: sampling faults.

➢ Higher than 150 MHz:

- First undetected fault windows appear.
- Injected faults:
  sampling faults + 1st timing faults.



➢ At 200 MHz:

- Close to the DUT max frequency no need for a strong EM stress to inject faults.
- Faults repeatability and properties match timing faults violation principle.
- Timing faults are undetected
  →Sensors have a short critical path.

➢ **Conclusion:**
- High detection of sampling fault model at low frequencies *(f<150 MHz)* by the current sensor.
- No detection of timing fault model obtained at high frequencies *(150 MHz ≤ f ≤ 200 MHz).*

➢ **Perspective:**
- Development of a new sensor that detects both fault models.
- Design should be suitable for FPGA and ASIC implementation.

Contact : roukoz.nabhan@emse.fr

Stakeholders

Authors

Roukoz Nabhan
Jean-Max Dutertre
Jean-Baptiste Rigaud
Jean-Luc Danger
Laurent Sauvage

ANR-20-CYAL-0007

Partners

Hardware implementation of LWC algorithm for connected objects

Parties prenantes

Institut Mines-Télécom

MINES Saint-Étienne

Une école de l'IMT

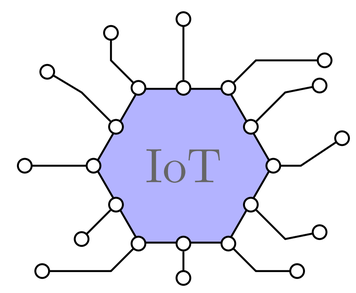
Auteurs

Nathan Roussel
Olivier Potin
Jean-Baptiste Rigaud
Jean-Max Dutertre

Partenaires

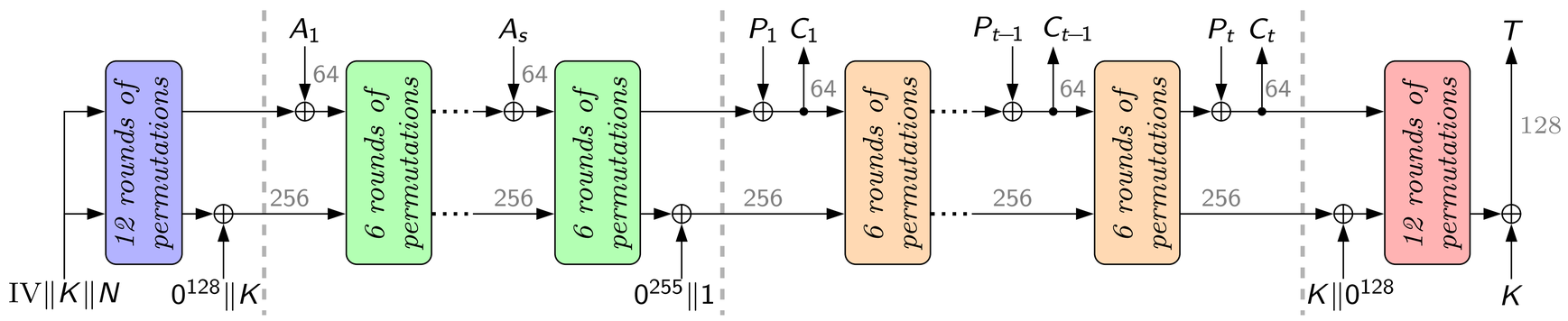
Context

- Microelectronics paved the way to Internet of Things (IoT)
- Low power, small area and security are IoT main constraints
- LightWeight Cryptography (LWC) algorithms are suitable to secure IoT applications
- Secure implementation of LWC to face physical attacks (side-channel or fault-based attacks)
- How to strengthen LWC algorithms with the lowest energy impact ?
- Hybridize Magnetic Random Access Memories (MRAM) and CMOS to adress this issue
- Power and security characterizations on reference CMOS implementation



Ascon : finalist of NIST LWC contest

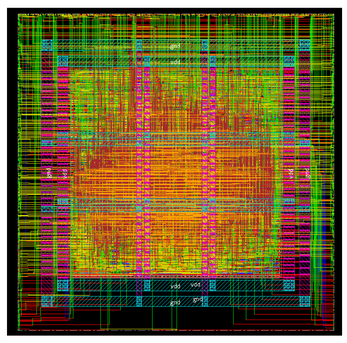
- **ASCON** : an Authenticated Encryption with Associated Data (AEAD) [1]
- Datapath of 320 bits divided into 5 parts of 64 bits each



ASCON-128

Reference CMOS implementation

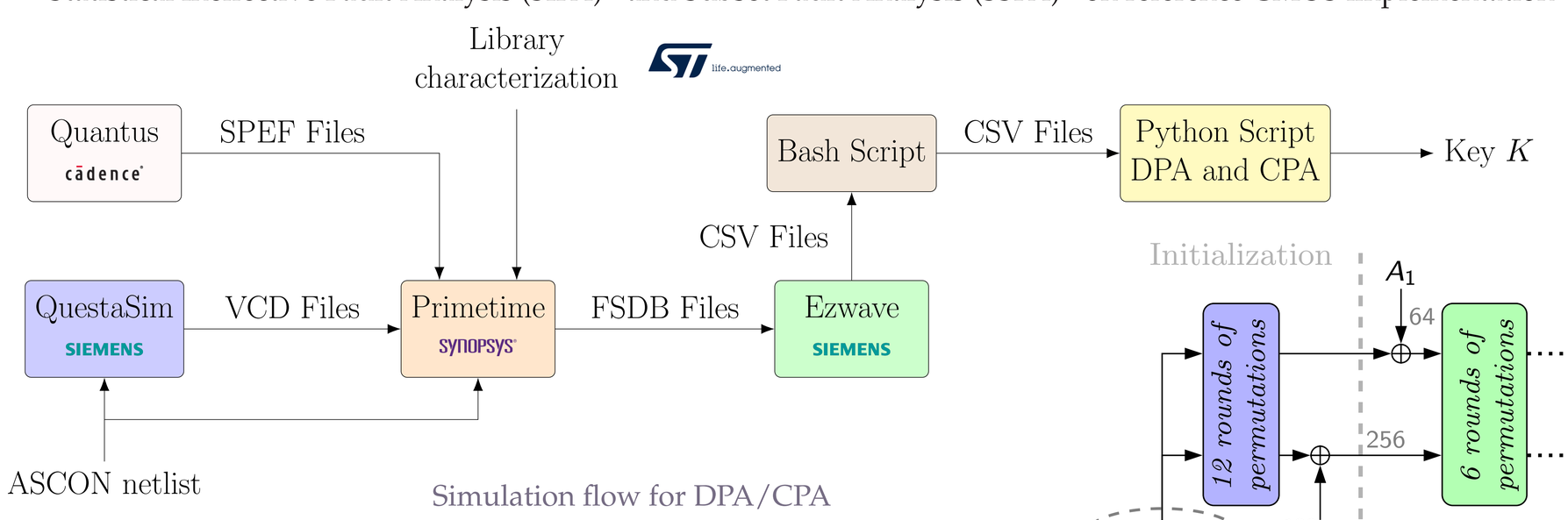
- CMOS conception flow with **28nm FD-SOI** technology from STMicroelectronics (CMP) :
  - VHDL description of the algorithm functional simulation with **ModelSim (Siemens)**
  - Synthesis with **Design Vision (Synopsys)**
  - Placement and routing with **Innovus (Cadence)**
  - DRC/LVS verifications with **PVS (Cadence)**
  - Parasitic extraction with **Quantus (Cadence)**
  - Power analysis with **PrimeTime (Synopsys)**
- Circuit area after placement and routing : **5000.6μm^2**
- Circuit power consumption after parasitic extraction : **798.9μW**
- Most ressource consuming part : **Intermediate state register**



Layout of ASCON

Security characterization

- Differential Power Analysis (DPA) [2] and Correlation Power Analysis (CPA) on reference CMOS implementation
- Statistical Ineffective Fault Analysis (SIFA) [3] and Subset Fault Analysis (SSFA) [4] on reference CMOS implementation



Simulation flow for DPA/CPA

Area of interest for DPA/CPA

1. C. Dobraunig et al., "Ascon v1.2 : Submission to NIST"
2. N. Samwel et al., "DPA on hardware implementations of Ascon and Keyak"
3. K. Ramezanpour et al., "A Statistical Fault Analysis Methodology for the Ascon Authenticated Cipher"
4. P. Joshi et al., "SSFA: Subset fault analysis of ASCON-128 authenticated cipher"

Acknowledgments

- This work is supported by the MISTRAL project (ANR-19-CE39-0010).
- MISTRAL is a collaborative research project
- MISTRAL is founded by the French National Research Agency (ANR).

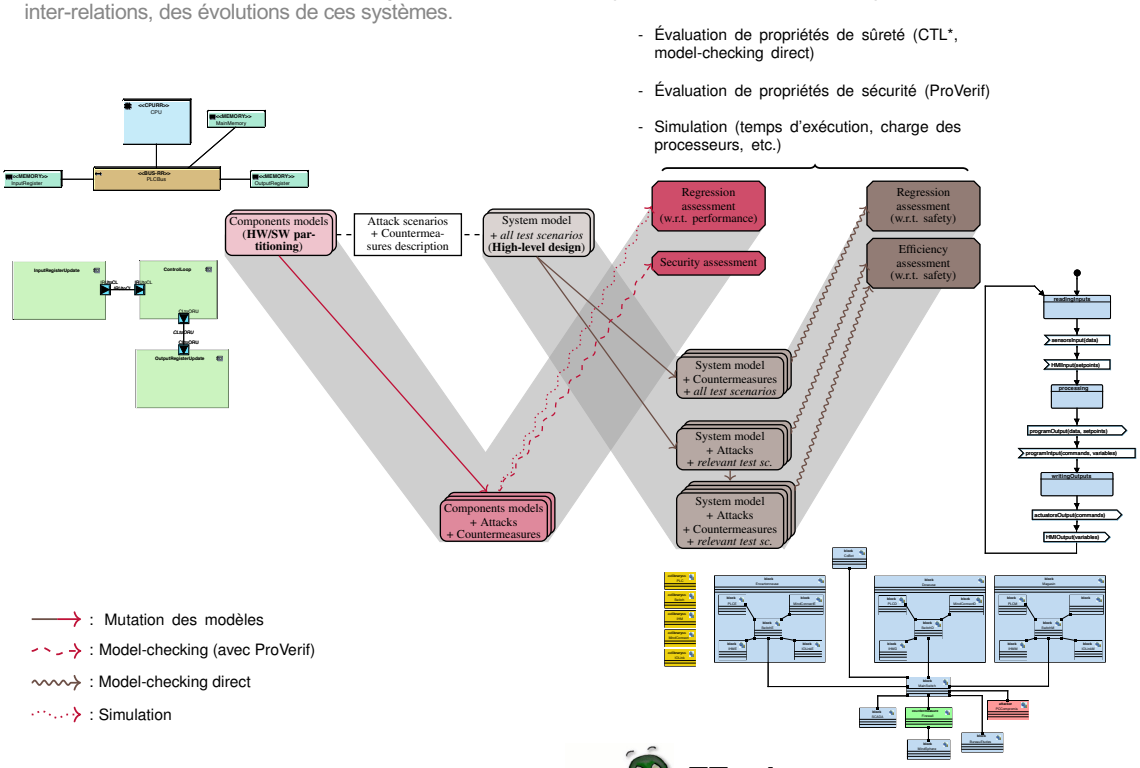
Contact : nathan.roussel@emse.fr

Institut Mines-Télécom

Cyber-sécurité de l'Industrie 4.0

W-Sec : une méthode innovante et formelle pour assurer la cyber-sécurité des systèmes industriels critiques pendant leur cycle de vie

L'industrie 4.0 s'appuie sur une numérisation et une connectivité fortement accrues de l'outil de production industriel. Les processus de maintenance des usines modernes doivent garantir leur sécurité numérique tout au long de leur cycle de vie, en plus de leur sûreté de fonctionnement et de leur performance. Ce projet de recherche vise à améliorer W-Sec, notre méthode d'évaluation conjointe et formelle des impacts de sûreté, sécurité et performance, et de leurs inter-relations, des évolutions de ces systèmes.



W-Sec

- Deux cycles de modélisation et de vérification : système/composants
- Estimation d'impact : vérification formelle assistée par la simulation
- S'appuie sur TTool

TTool

- Outil intégré de modélisation, de vérification formelle et de simulation
- Open-source, développé par le LabSoC depuis 2004
- https://ttool.telecom-paris.fr

Terrain de recherche : IT'm Factory

IT'm Factory est l'atelier pilote « industrie du futur » de l'École des Mines de Saint-Étienne pour la recherche, l'enseignement ou la formation en lien avec la transition numérique de l'industrie.

- **Atelier** : un bureau d'études, un datacenter, deux chaînes de production.
- **Cas d'étude** : chaîne de conditionnement.
- **Objectifs** : automatiser les mutations des modèles dans W-Sec, expliciter les liens sémantiques entre les deux cycles, implémenter le support de W-Sec dans TTool.
- **Résultats préliminaires** : identification de vulnérabilités et conception de scénarios d'attaque liés à des évolutions fonctionnelles, premiers modèles.

Parties prenantes

TELECOM Paris · IP PARIS · MINES Saint-Étienne — Une école de l'IMT

Auteurs

Ludovic Apvrille - TP
Philippe Jaillon - MSE
Bastien Sultan - TP

Partenaires

INSTITUT CARNOT Télécom & Société numérique
INSTITUT CARNOT M.I.N.E.S
SPARTA

Contacts :
ludovic.apvrille@telecom-paris.fr

bastien.sultan@telecom-paris.fr

philippe.jaillon@emse.fr

Projet financé dans le cadre de l'interCarnot M.I.N.E.S – TSN 2022

Evaluating the cost of beyond AES-128 LoRaWAN security

Parties prenantes

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

Université de Mons

Auteurs

Phithak THAENKAEW
Bruno QUOITIN
Ahmed MEDDAHI

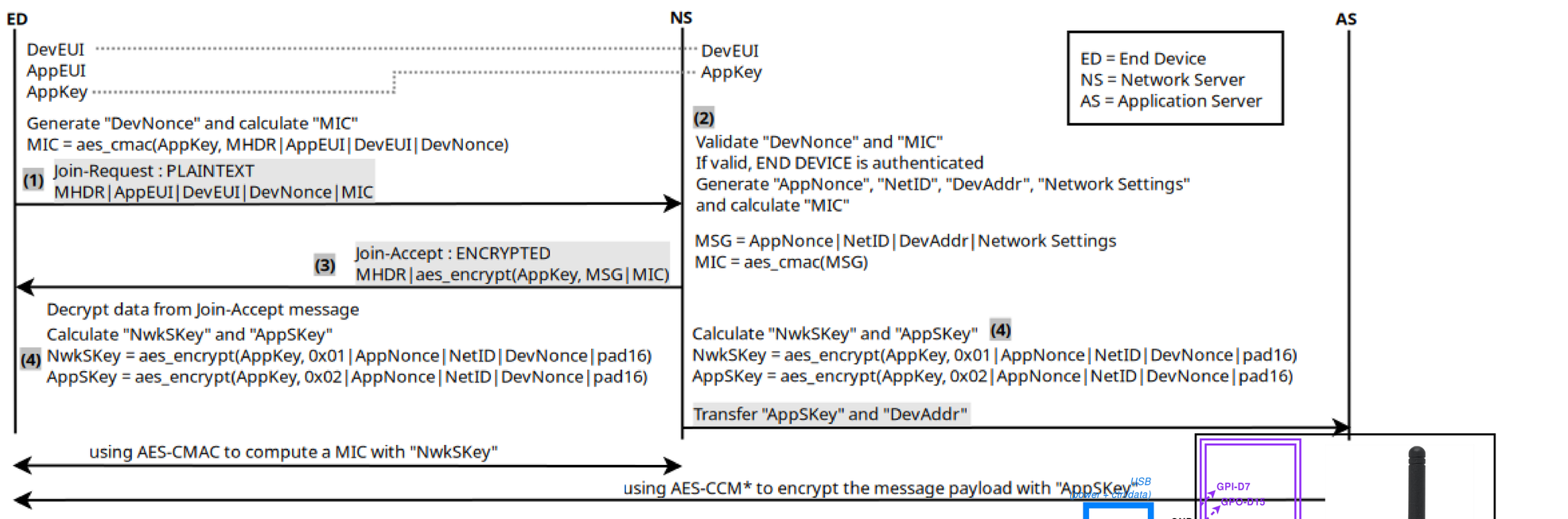
Partenaires

a member of NSTDA

Context and Problem:

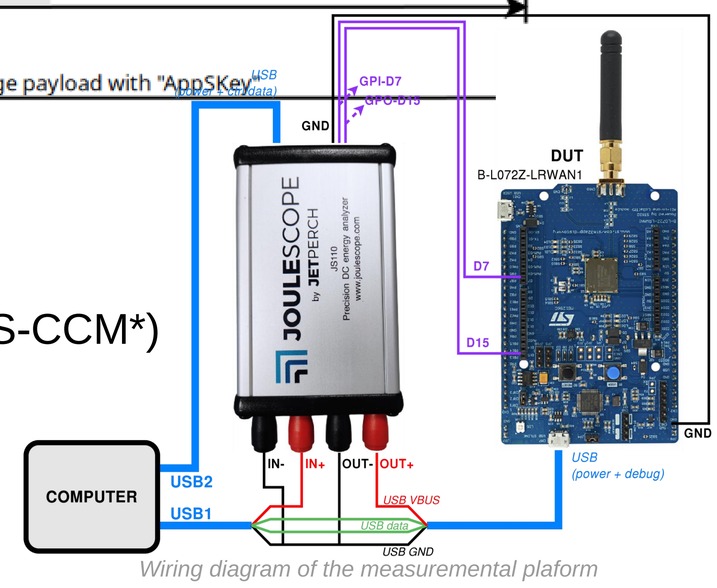
- **AES-128**, symmetric key, is used for **LoRaWAN** communication encryption in :
  - Device activation via Over-the-Air Activation (OTAA)
  - Messages encryption between End-Devices and Servers and MIC calculation
- Issue with AES-128 :
  - Not strong enough today due to increased **computing power** and the advent of **quantum computing**
  - **Grover's algorithm** can be applied to break AES 128 with 2,953 qubits while the number of qubits to make such attack practical trend is expected to be reached in the near future

➢ Exploring impact of longer keys (192 or 256 bits) on **processing time** and **energy consumption**

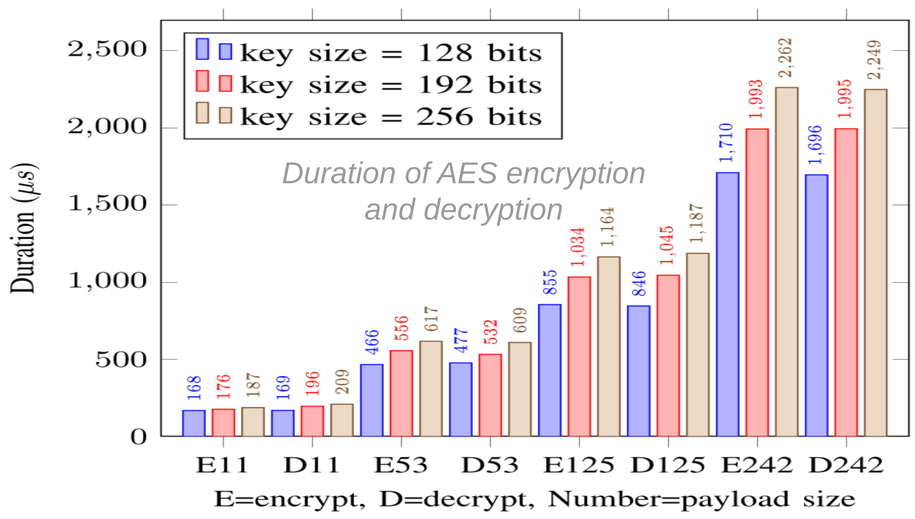


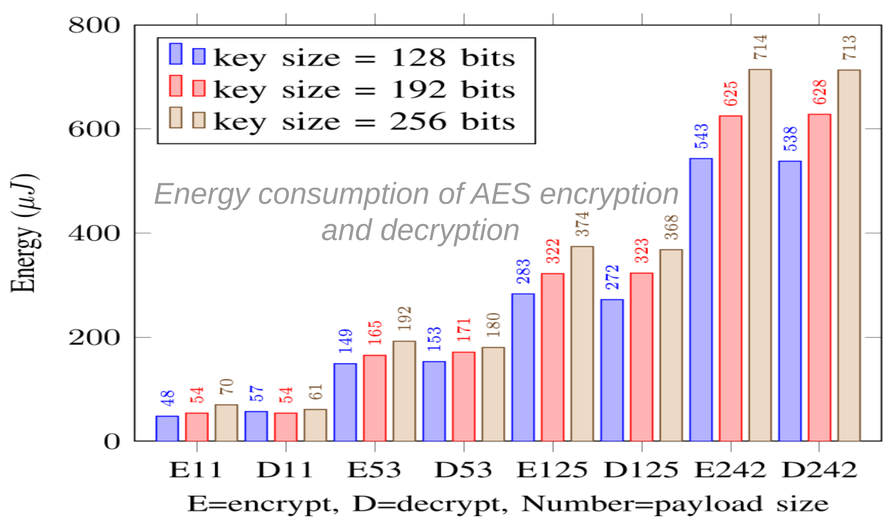
Experimental Results

- Measuring **processing time** and **energy consumption**
- Three **functions** : encrypt_payload, decrypt_payload (AES-CCM*) and compute_mic (AES-CMAC)
- Three AES **key sizes** : 128, 192 and 256 bits
- Four **payload sizes** : 11, 53, 125 and 242 bytes



Wiring diagram of the measuremental plaform





➢ The **longer** of the **key size** has a **limited impact** on the **energy consumption** of the device

Future Works

- Implement the **longer key** size of AES to LoRaWAN network
- Consider the use of stronger authentication with **asymmetric cryptography** and certificates by relying on Elliptic-Curve Cryptography (ECC)
- Other communication protocol would be integrated to the testbed platform (e.g. SCADA)
- Cross layer approach for a lighweight autentication and identification of the device

……..

Contact : phithak.thaenkaew@umons.ac.be

GASP : a Generic Approach to Secure Protocols

Projet ANR JCJC 2019

Les protocoles réseau sont omniprésents dans nos échanges quotidiens. Les vulnérabilités affectant ces briques de base de nos systèmes peuvent avoir des conséquences graves (p. ex. Heartbleed, FREAK). Pour améliorer leur sécurité, GASP vise à automatiser l'implémentation et l'évaluation des piles protocolaires.

Mars 2022 Colloque de l'Institut Mines Telecom Palaiseau

Parties prenantes

TELECOM SudParis

IP PARIS

Auteurs

Olivier Levillain (porteur)
Aina Toky Rasoamanana

Financement

anr

CONTEXTE ET OBJECTIFS

Les protocoles réseau d'aujourd'hui sont omniprésents et d'une grande complexité. Il est donc compliqué de les implémenter de manière fiable et sécurisée.

Exemple de vulnérabilités liées aux implémentations TLS

- Heartbleed (divulgation d'informations sensibles) ;
- FREAK (vulnérabilité de la machine à états) ;
- Berserk (usurpation serveur via des signatures contrefaites).

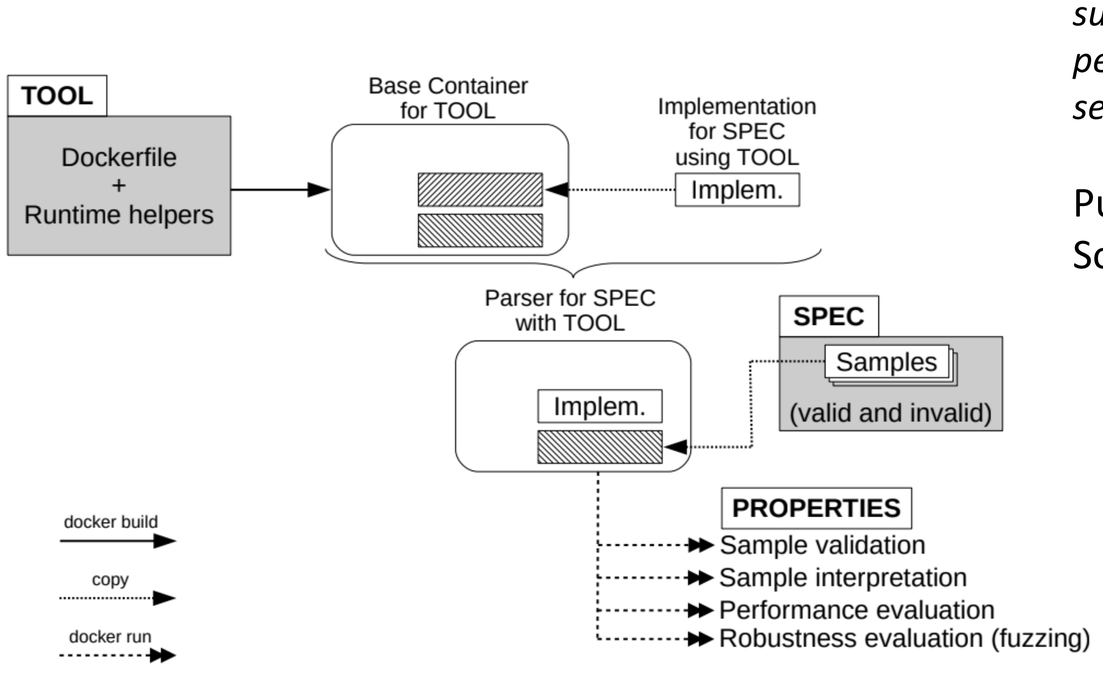
GASP propose trois axes pour d'amélioration

- La génération automatique des *parsers* à partir d'une description dans un langage dédié (DSL) ;
- La génération automatique d'implémentations à partir d'une description dans un langage dédié ;
- L'analyse en boîte noire d'implémentations existantes pour détecter des défauts dans les machines à état.

MÉTHODOLOGIE ET RÉSULTATS

Étude des générateurs de *parsers* à l'aide d'une plateforme comparant l'expressivité, la robustesse et la performance.

Langsec-PF est une plateforme intégrant des outils (Hammer, Kaitai-Struct, Nail, Nom, Parsifal) via des conteneurs Docker.

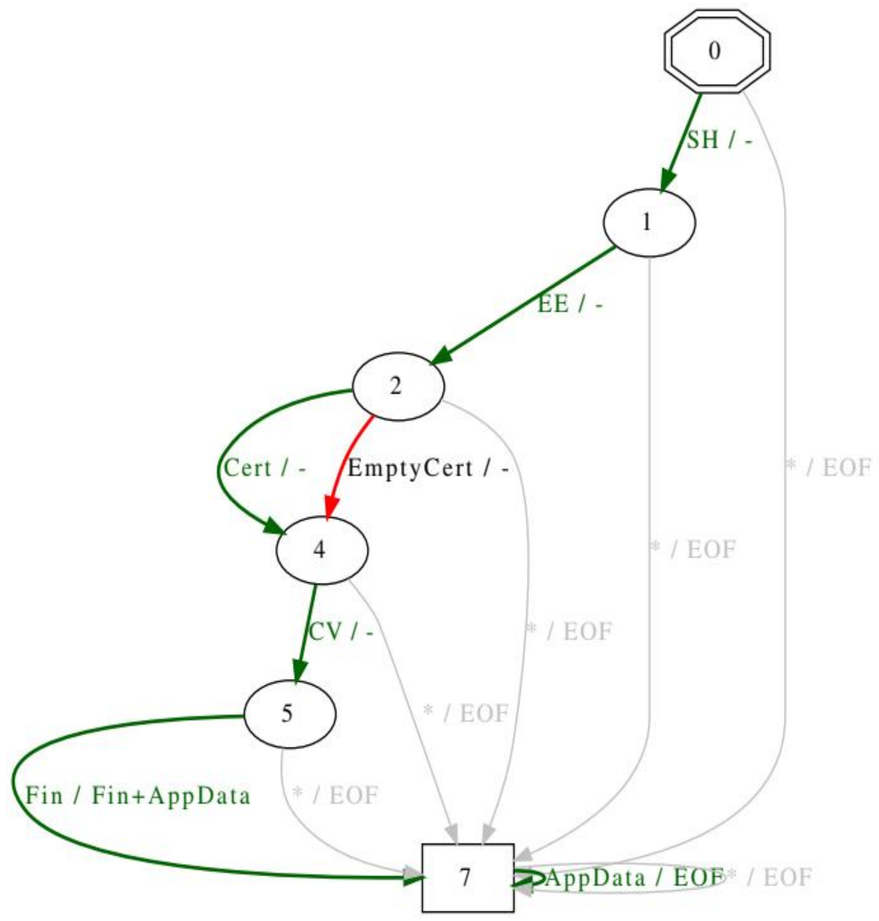


Dépôt : https://gitlab.com/pictyeye/langsec-pf (logiciel libre)
Publication : Naud, Levillain et Rasoamanana - *Towards a Platform to Compare Binary Parser Generators* - LangSec 2021

Analyse des machines à états par inférence en boîte noire d'implémentations existantes, avec application à TLS et SSH

TLS Inferer est un outil pour inférer la machine à état d'implémentations en utilisant l'algorithme L*.

Exemple de vulnérabilité mise au jour dans wolfssl (CVE-2021-3336) : contournement de l'authentification serveur dans les clients TLS 1.3.



La figure décrit la machine à état du client TLS 1.3 de wolfssl (versions antérieures à 4.7). La transition en rouge, suivie d'un message CV (CertificateVerify) arbitraire, permet à un attaquant de contourner l'authentification du serveur.

Publication prochaine de l'outil
Soumission des résultats en cours

Travaux à venir sur la génération d'implémentations, par généralisation des travaux sur TLS et SSH.

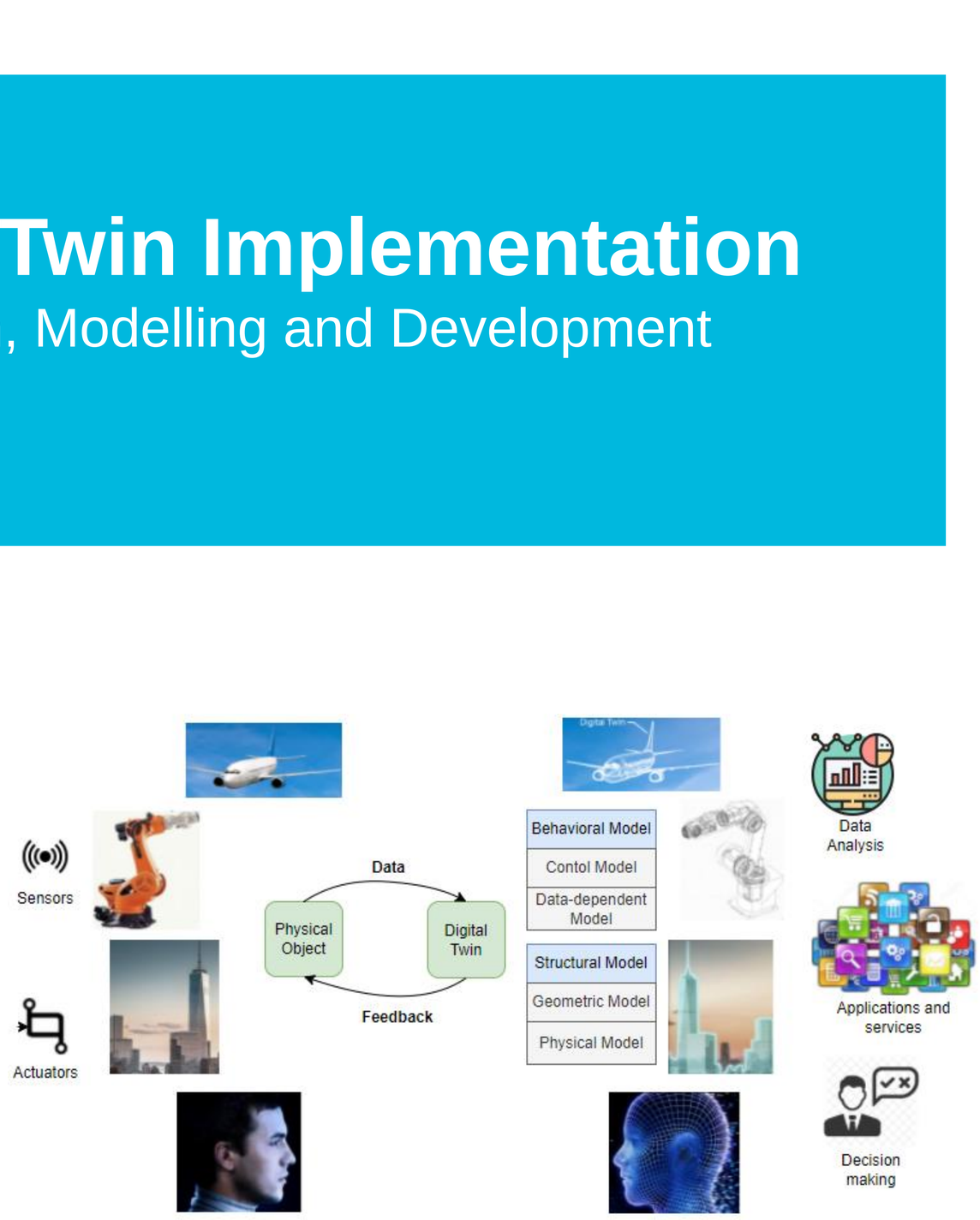
Contact : olivier.levillain@telecom-sudparis.eu

Digital Twin Implementation

Conception, Modelling and Development

What is a Digital Twin (DT)?

- A DT is a software representation of a physical system.
- It uses models to reproduce its structure, behavior and conditions.
- DT can be used to design, develop, simulate, monitor, and optimize the real system.
- It is composed of three main components
  - **Physical Object**
  - **Virtual Object**
  - **Data Synchronization**



Digital Twin

A Survey to Implement DT

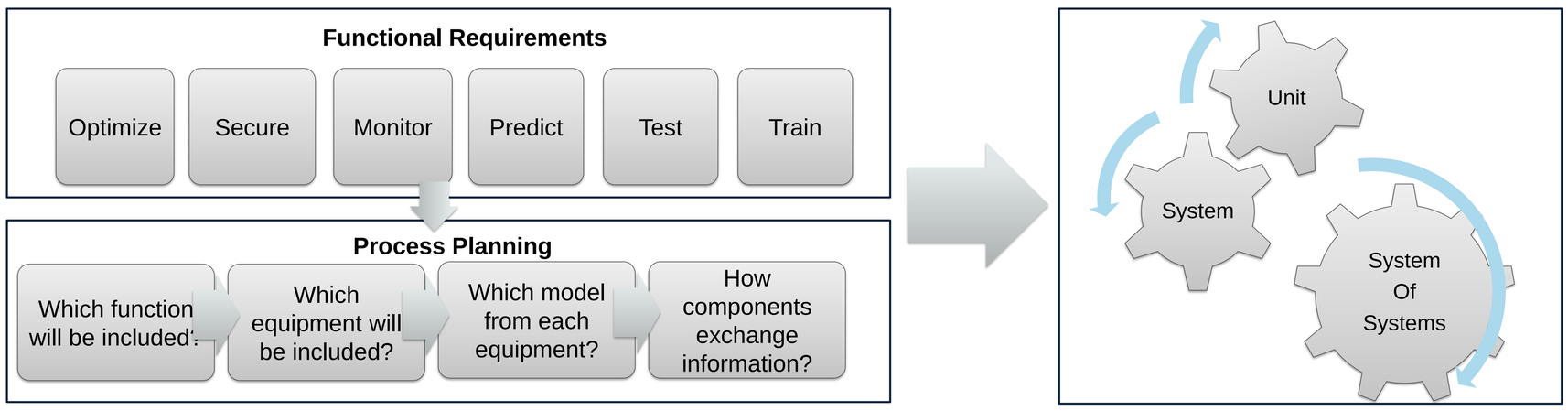
Implementation Techniques and Procedures

Digital Twin Conception
- Functional Design
- Architecture Design

Digital Twin Modeling
- Model Design
- Integration and Verification

Digital Twin Development
- Experimental Platfrom
- Data Synchronization

Conception



Functional Design

Architecture Design

Modeling

Physics-based

Mathematical models based on the laws of physic

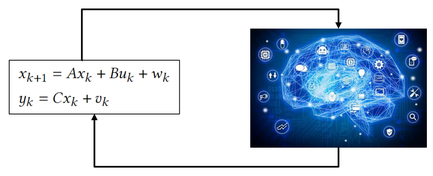
$$x_{k+1} = Ax_k + Bu_k + w_k$$
$$y_k = Cx_k + v_k$$

Data-based

Artificial Intelligence algorithms to create a model

Hybrid

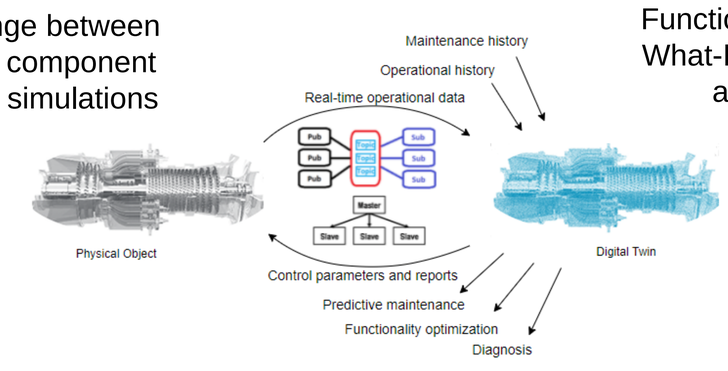
Combines Physics and Data-based approaches



Development

Real-Time Synchronization

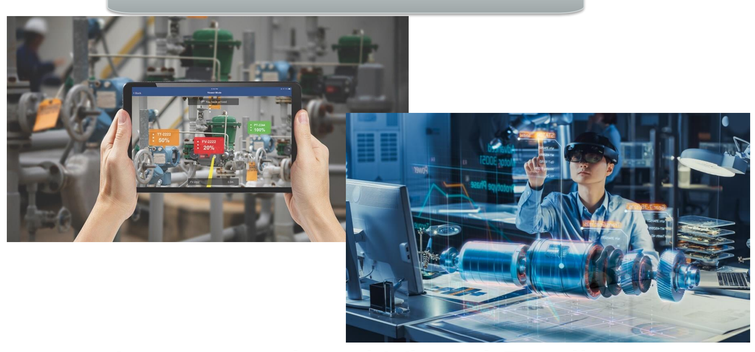
Data exchange between the physical component and the twin simulations



Moving Target Defense

Functional, Stress and What-If Testing of new approaches

Mixed Reality



Augmented and Virtual Reality

Authors

Zeinab RAHAL
Mariana SEGOVIA
Joaquín GARCIA-ALFARO

Détection d'intrusion pour des réseaux embarqués automobiles

Approches d'apprentissage profond pour une meilleure détection

Institut Mines-Télécom

Parties prenantes

TELECOM Paris

IP PARIS

Auteurs

Natasha Alkhatib
Maria Mushtaq
Hadi Ghauch
Jean-Luc Danger

Partenaires

NOKIA

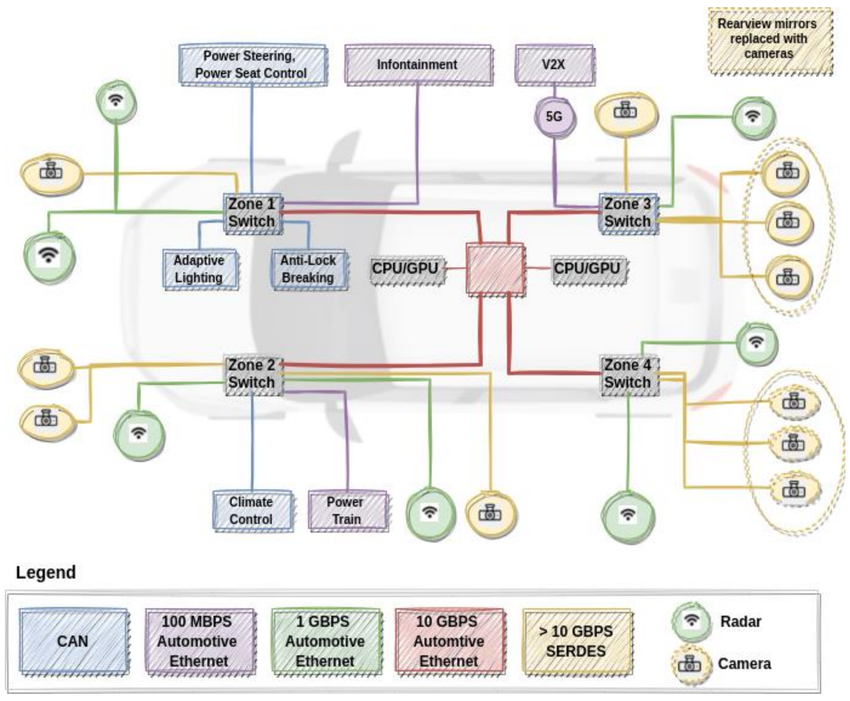
THALES

Valeo
SMART TECHNOLOGY FOR SMARTER CARS

WAVESTONE

Contexte

- **Assurer la sécurité et le divertissement** – des services sophistiqués sont mis en place par les constructeurs automobiles.
- **Complexité croissante des logiciels embarqués** – augmentation de la probabilité d'apparition des vulnérabilités dans ces logiciels.
- **Connectivité étendue des véhicules** – multiplication des interfaces de communication entre le réseau interne et le monde extérieur.
- **Cyberattaques automobiles** – plus de points d'entrées sur les réseaux automobiles embarqués (CAN, FlexRay, MOST, LIN et Ethernet).
- Ces réseaux puissent contenir des vulnérabilités qu'un attaquant peut exploiter.



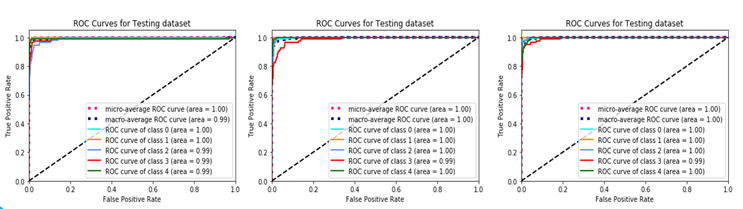
Objectifs

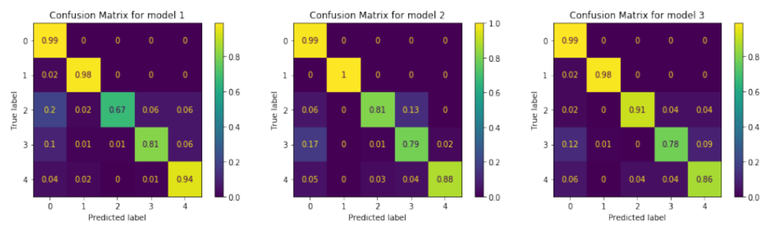
Dans cette thèse, nous utiliserons des techniques d'apprentissage profond pour détecter des intrusions à l'intérieur des différents types de réseaux automobiles embarqués.

- **Données** – Générer et utliliser des ensembles de données contenant différents types s'intrusions sur divers réseaux automobiles embarqués, en particulier Automotive Ethernet (SOME/IP et AVTP) et CAN.
- **Approches basées sur les données** – Construire et comparer différentes techniques de détection d'intrusion supervisées et non supervisées pour la détection d'intrusion en termes de performances et de compléxité de calcul.
- **Solution en temps réel** – Embarquer notre solution dans un calulateur ECU et vérifier son efficacité en temps réel.

Détection supervisée de divers types d'intrusion sur le protocole SOME/IP

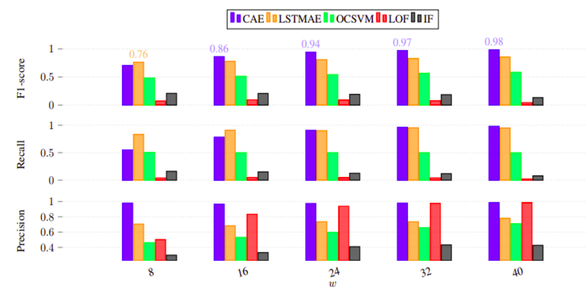
- **Créer une base de donnée composée de traces de paquets SOME/IP normales et anormales.**
- **Développer un modèle supervisé de réseau neuronal récurrent (RNN) pour classer différents types d'attaques.**
- **Divers types d'Intrusions prédites avec succès avec des valeurs F1 et AUC supérieures à 0.8.**





Comparaison de differents techniques non supervisée de détection d'intrusions sur le protocole AVTP

- **Les méthodes deep learning (Autoencoders) vs machine learning.**
- **Meilleure modèle CAE pour différents longueurs de séquences AVTP (0,76<score F1<0,98 et temps de détection = 0.4 s)**



Réference:.

Alkhatib, Natasha, Hadi Ghauch, and Jean-Luc Danger. "SOME/IP Intrusion Detection using Deep Learning-based Sequential Models in Automotive Ethernet Networks." 2021 IEEE 12th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2021.

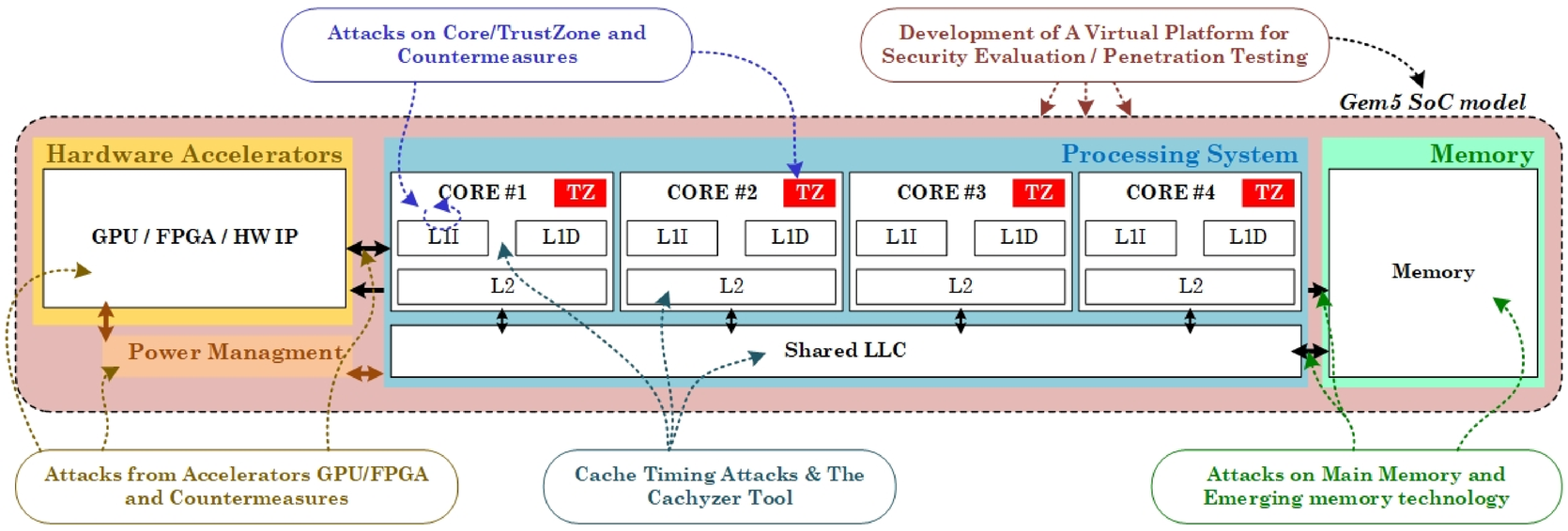
Contact : natasha.alkhatib@telecom-paris.fr

Projet: https://github.com/Alkhatibnatasha/SOMEIP_IDS

ANR - ARCHISEC

Virtual Platform to Analyze the Security of a System on Chip at Microarchitectural Level

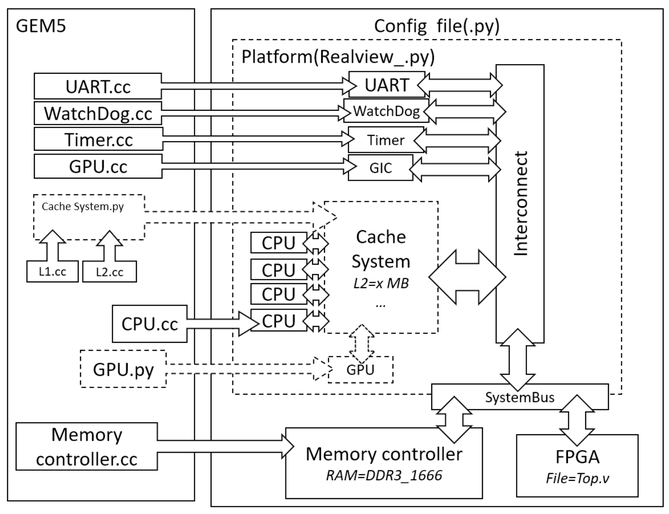
Contact : quentin.forcioli@telecom-paris.fr



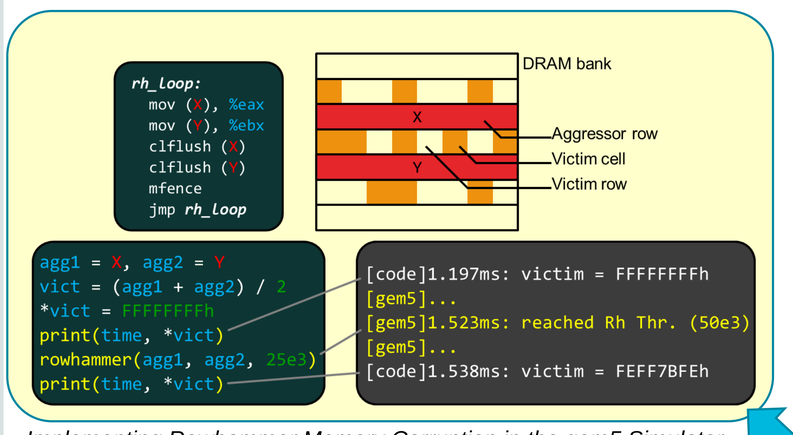
SoC heterogeneity : multiple attack vectors

Cybersecurity is also an hardware issue

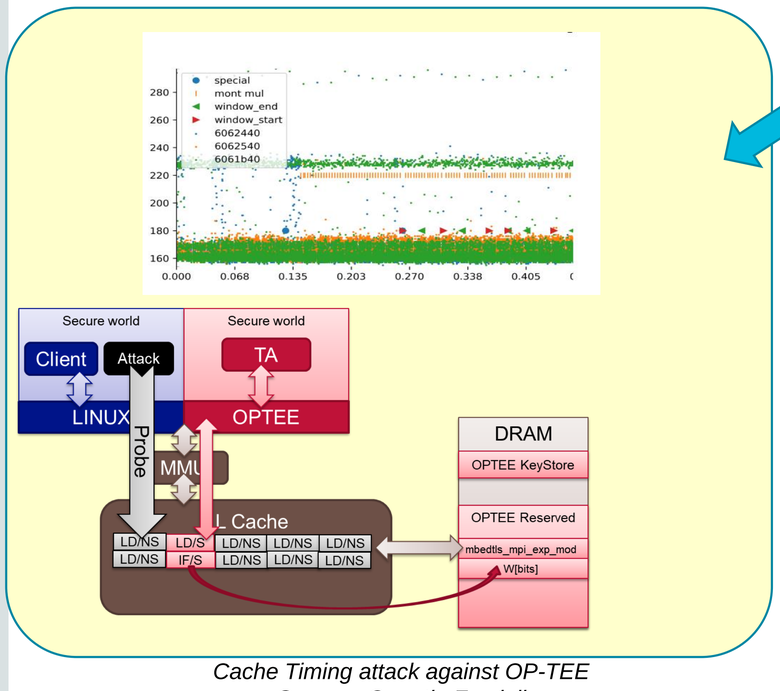
- ► **Prime+Probe & Flush+Reload** *(Target : Cache)* – Information leaks through cache as a side channel
- ► **Spectre/Meltdown** *(Target : Predicter)* – Arbitrary code execution to cause cache side effect,
- ► **Rowhammer** *(Target : DRAM)* – Triggering bitflip in victim memory causing unintended behavior.
- ► **Programmable devices** *(ex:GPU/FPGA)* – Other possible attack vectors.
- ► **Covert channel** *(ex:DVFS)* – Using a side-channel to hide a communication between isolated tasks
- ► **Trusted Execution Environment** *(TEE)* – Provide an API for secure operation using secure hardware primitives



how the gem5 simulator is structured
Source : Quentin Forcioli



Implementing Rowhammer Memory Corruption in the gem5 Simulator
Source : Loïc France et al.



Cache Timing attack against OP-TEE
Source : Quentin Forcioli

Simulation for security evaluation

SoC Simulation platform :

- ► **gem5** : open-source simulator
  - SoC Simulator : *config base customization that allow to interconnect different element to memory buses,*
  - Timing simulation (Cache, DDR controller, …)
  - Multiple CPU model : *Out of order, in order, minimalist; with their effect on timing.*
  - SystemC simulator : FPGA/ASIC simulation
  - Multiple ISA support (including ARM), GDB support, Pipeline visualization,…
- ► **Templates :** We are also providing template projects for using gem5,

Building our platform

From Tools & Example to Results :

- ► **Improvement to gem5** :
  - Ramulator : *Accurate ram simulator, improved by taking rowhammer effect into account*
  - OP-TEE support : *Open source TEE relying on Arm TrustZone*
- ► **Attack PoCs on gem5:**
  - Basic Cache timing and Spectre attack : *Flush+Reload and Spectre-PHT on gem5 (tested on real hardware).*
  - Rowhammer attack : *leveraging our Ramulator implementation*
  - DVFS cover channel : *using gem5 DVFS implementation*
  - TEE hash signing scenario : *PoC of cache-timing attack in development*
- ► **Tools :** Cachalyzer *(Cache static analylzer)*

Parties prenantes

Auteurs

Quentin Forcioli
Jean-Luc Danger
Clémentine Maurice
Lilian Bossuet
Florent Bruguier
Maria Mushtaq
David Novo
Loïc France
Pascal Benoit
Sylvain Guilley
Thomas Perianin

Partenaires

Menaces sur les services à faible latence

Le cas de l'architecture L4S

Institut Mines-Télécom

Parties prenantes

MOS AICO

- PROJET FINANCÉ PAR L'ANR - PROJECT FUNDED BY THE ANR
ANR

Auteurs

Marius Letourneau
Boris N'Djore Kouame
Guillaume Doyen
Bertrand Mathieu
Rémi Cogranne

Partenaires

orange™

montimage

Loria
Laboratoire lorrain de recherche en informatique et ses applications

utt
UNIVERSITÉ DE TECHNOLOGIE
TROYES

Contexte – De nouveaux services à fortes exigences de latence

Les sources de la latence

► **Temps de traitement** – Temps de traitement des entités terminales et des équipements intermédiaires (*middleboxes*)

► **Temps d'acheminement des données dans le réseau:**

- La **taille des files d'attentes**
- La **réactivité à la congestion**

Les solutions

► **Active Queue Management** (*AQM*)

► Nouveaux algorithmes de **contrôle de congestion**

► **Explicit Congestion Notification** (*ECN*)

Exemple de services faible latence envisagés: Industrie connectée, Cloud Gaming, Pilotage de drones et Véhicules Autonomes

Une solution architecturale standardisée par l'IETF

The Low Latency, Low Lass and Scalable throughput (L4S)

Principes généraux

► **Réactivité**
Double file d'attente à probabilités de signalement différenciées

► **Cohabitation**
Couplage des deux files pour isoler partiellement leur performance

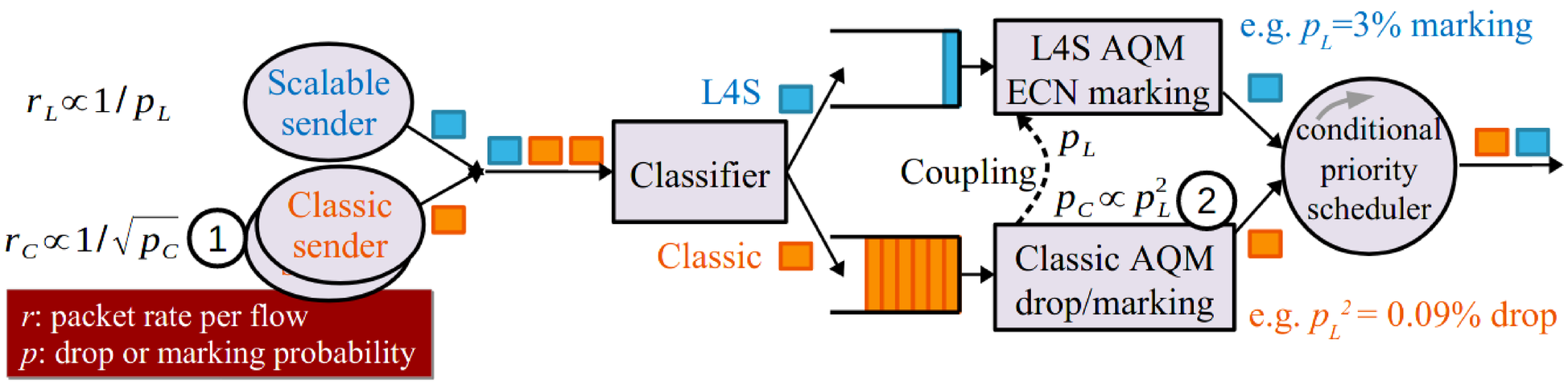
Couplage des AQMs

► **Probabilités de signalements**

► **Isolation** entre flux classiques (*C*) et faible latence (*L*)

► **Réactivité** adaptée au degré de congestion

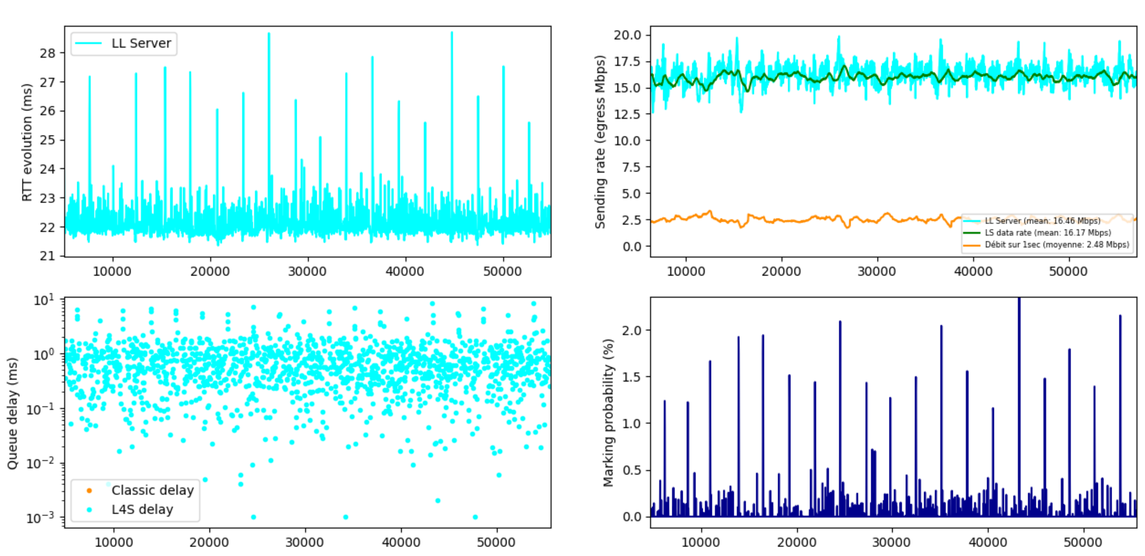
► Prévient la **famine** de (*C*)



Netdev 0x13, 2019
Source : Implementing the « Prague Requirements » for L4S

Problématique – Menaces sur la latence liée à la conception de l'architectureL4S

Exemple de caractérisation d'une des menaces



Impacts d'un flux indésirables (bursts de connexion) sur un flux faible latence légitime *Sont représentés: le RTT du flux légitime, le débit du flux légitime et le débit attaquant, le queuing delay de la file (L), la probabilité de marquage source*

Les bursts de connexion

► Génération de **bursts de téléchargement** d'un fichier de 800ko

► Débit en sortie de routeur de **20Mbps**

► **Modification** *user-space* de la **couche transport**

► Un **client légitime subit 5ms de délai** avec pourtant un **très faible débit d'attaque**

Contact : marius.letourneau@utt.fr

Mars 2022 Colloque de l'Institut Mines Télécom Paris

Résilience et protection des données

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

CHAIRE CYBER CNI
Sécurité des infrastructures critiques

Software-defined Security for Network Function Virtualization

Author

Manel Smine

Phd Student
3rd year
2022

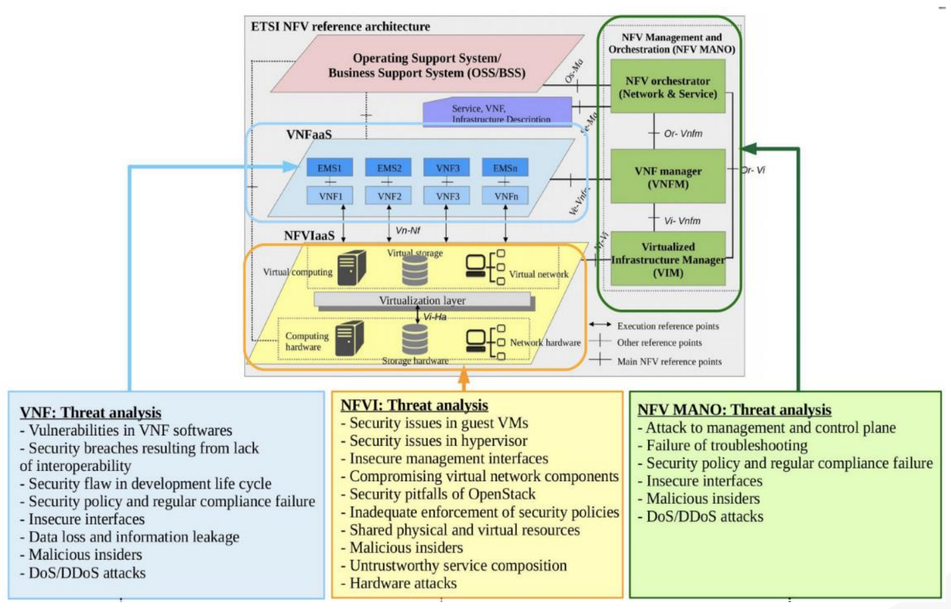
Advisors

Marc-Oliver Pahl
David Espes

School

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Context: NFV Security



Motivation:

Enhancing the security of NFV services by defining an optimal deployment of access control policies

Research Questions:

How to deploy access control policies on NFV services?

- How to specify high-level access control requirements to be enforced over network services?
- How to transform the high level access control policy into a concrete deployable policy?
- How to efficiently manage conflicts and exceptions that may exist between different access control policies?
- How to optimally deploy of access control model on NFV services?

Contributions:

1. Network Functions Virtualization Access Control as a Service:

- **Formal high-level specification** of access control requirements to be enforced
- **Generic:** can deploy most types of access control policy such as RBAC, ABAC,…
- **Provably correct** method for transforming the high-level access control requirement towards a domain type enforcement (DTE) specification.
- **Efficient** enforcement method.

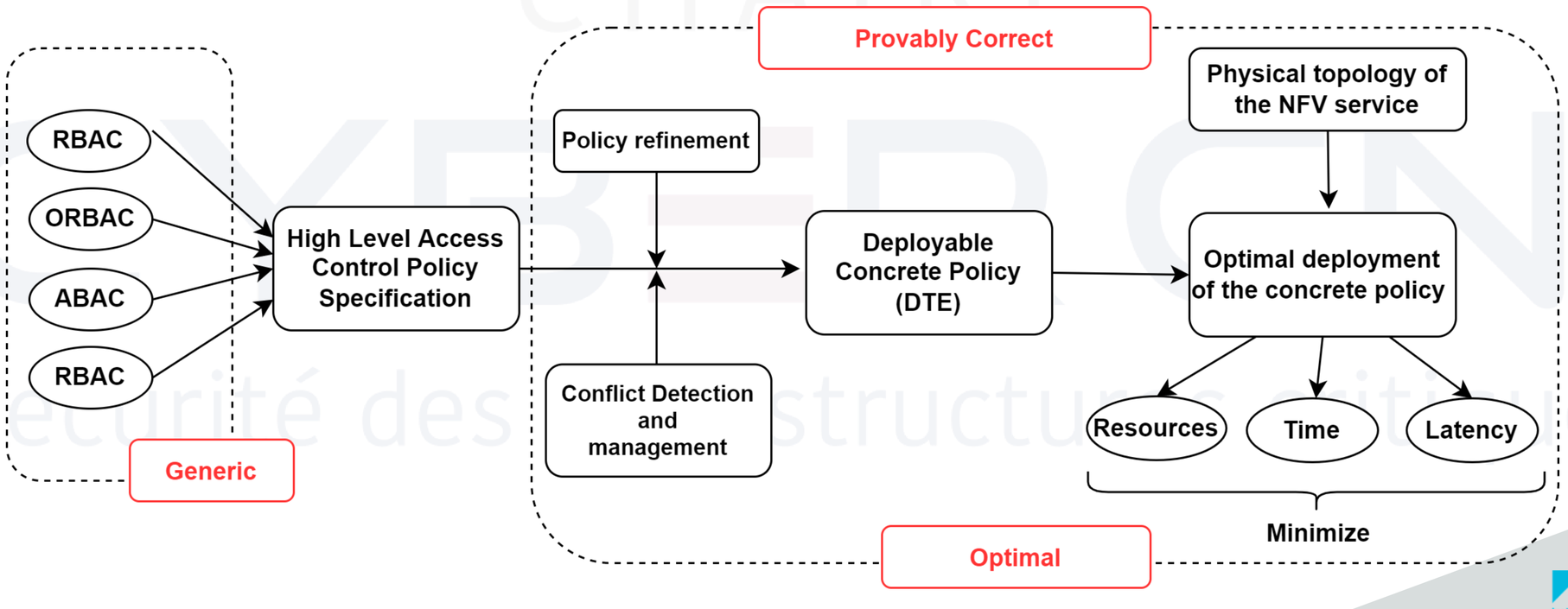
2. Exception Management:

- **Efficiently** enforce **complex access control** policies containing **exceptions** and / or **conflicting rules** on NFV services
- Propose a **provably correct** priority-based DTE access control model

3. Optimal Access Control Deployment in Network Function Virtualization:

- **Formal modeling** that allows to **model, quantify and optimize** the **resources** consumed and the impact in terms of **latency**
- **Correct** and **optimal deployment** of access control policies on NFV services

Current Work: dynamic deployment of access control policies on NFV services



Contact: **manel.smine@imt-atlantique.fr**

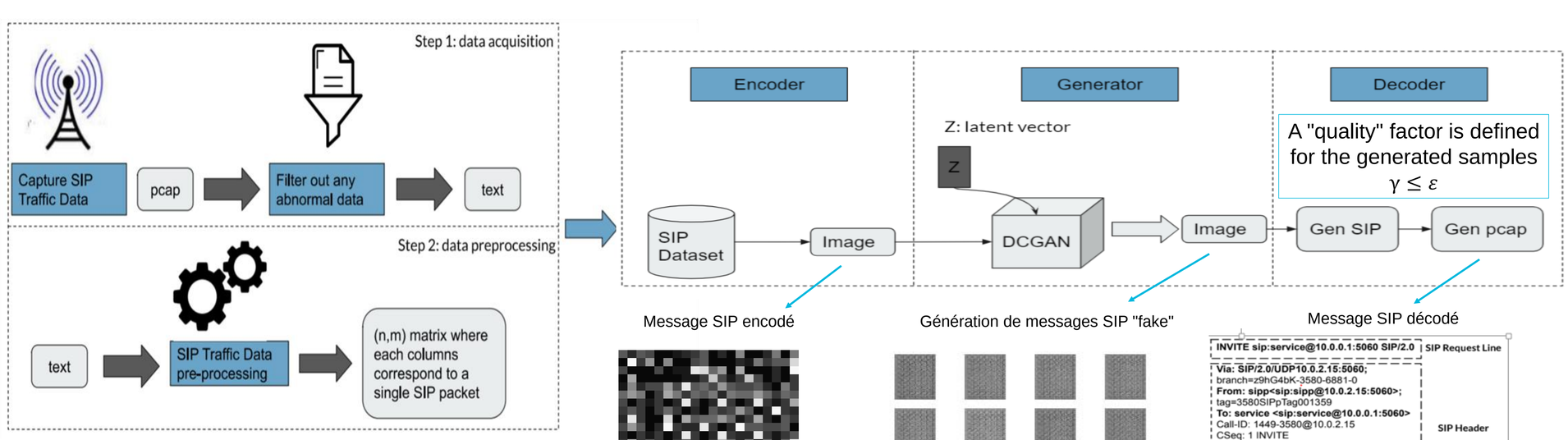
SIP-GAN: Generative Adversarial Networks for SIP traffic generation*

Problem:

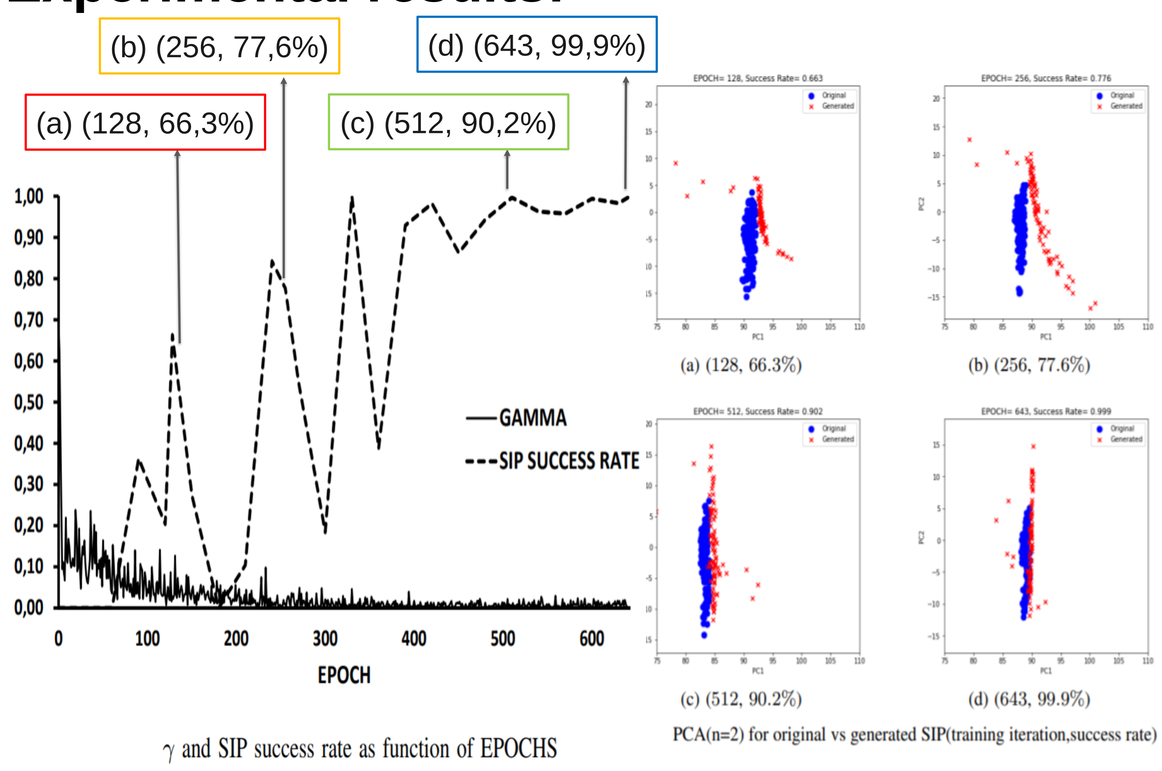
Generative adversarial networks (GANs) are one of the major ML techniques for data augmentation and classification, in the field of image processing, computer vision and natural language processing. However, in the field of data networks and protocols the use of GANs for data generation and classification (at packet level) is very limited or relatively new. GANs specific properties and characteristics can be highly relevant in this context (unsupervised technique). This limitation, is even more critical if we consider network protocols or communication oriented protocols (ex. SIP VoIP)

Proposition:

”SIP-GAN” to extend and adapt GANs model for SIP, aiming to process and generate SIP traffic at packet level. The proposed generic model includes an encoder, a generator, and a decoder. The encoder extracts information from pcap data, associates and converts these SIP data into a GAN image representation. The generator is based on a DCGAN model, that generates new SIP dataset from each extracted image. The decoder combines the generated images and reconstruct a valid pcap file (SIP file). A specific testbed, with a formal and practical analysis, demonstrate the validity of the generated data, from the SIP-GAN model.

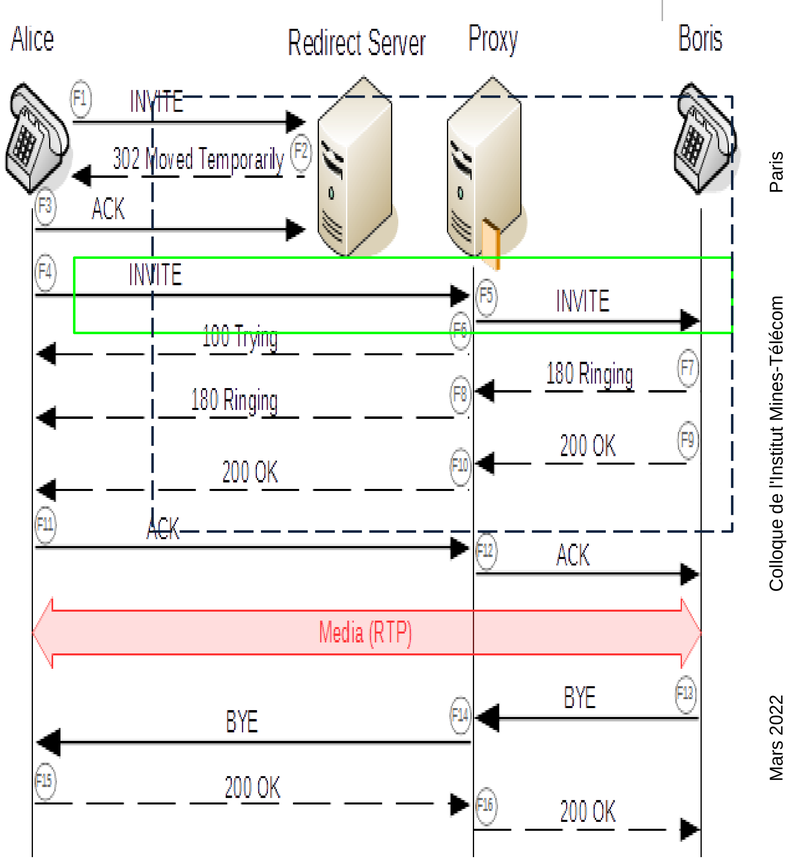


Experimental results:



γ and SIP success rate as function of EPOCHS

PCA(n=2) for original vs generated SIP(training iteration,success rate)



Perspectives and future works:

-Generate more complex scenarios
-Generate different SIP attack scenarios (ex. SIP fake register, fake bye, SIP DOS...)
-Identify and classify the SIP traffic behavior ("normal" and "abnormal")
…….

*Amar Meddahi, Hassen Drira, Ahmed Meddahi, ISNCC-2021 AIML, UAE, Oct. 2021

Contact : amar.meddahi@etu.inp-n7.fr

Parties prenantes

IMT Nord Europe
École Mines-Télécom
IMT-Université de Lille

Auteurs

Amar MEDDAHI
Hassen DRIRA
Ahmed MEDDAHI

Partenaires

Secure data storage into DNA molecules compliant with biological constraints

Ensuring the confidentiality of data stored into DNA molecules

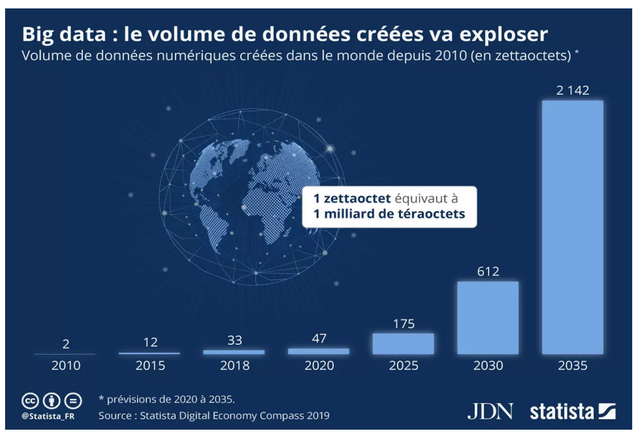
Parties prenantes

IMT Atlantique
Bretagne-Pays de la Loire
École Mines-Télécom

Auteurs

Chloé Berton
Gouenou Coatrieux
Dominique Lavenier

Partenaires



Volume of data created or replicated in the world, projection for 2020 to 2035 - Source : Statista

Considering the security of a promising storage medium

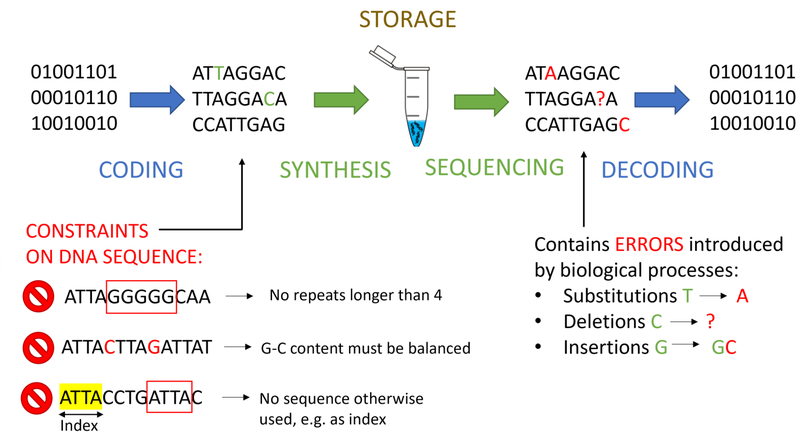
Introduction and motivation

- **Context** – Actual storage technologies (flash memory, hard drives, magnetic tapes,..) are outpaced by the exponential rise of digital data production [1]
- **Advantages of DNA storage [2]** – Density of 10^{21} bytes in one gram (10^6 times more compact than hard disks), durability for centuries, energy cost close to zero (molecules kept at room temperature with no maintenance)
- **Motivation** – Introducing security to ensure the confidentiality of the data stored into DNA molecules

A new data storage medium

DNA data storage

- **Principle** – [**WRITING**] Encode binary data into 4-base sequences following the DNA structure, transfer this data into synthetic DNA molecules. [**READING**] Amplify encoded sequences of interest and get several reads of them with a sequencing device. Reads are then processed and decoded back to binary data
- **Constraints** – i) Biological DNA synthesis and sequencing are imperfect and introduce errors. ii) devices have structural DNA requirements when generating 4-base sequences
- **Vulnerabilities** – This chain is notably vulnerable to: theft or cloning of molecules; spying attacks on the sequencing or synthesis devices; DDoS attack by adding fake DNA sequence to confuse sequencing



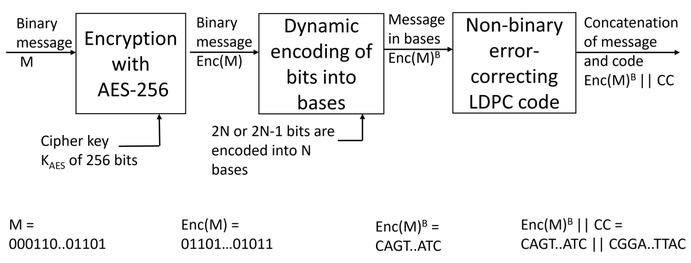
Data is UNPROTECTED in the storage chain, vulnerable to spying attacks or theft

DNA-based data storage chain, including the constraints on the structure of DNA sequences to store, and types of errors caused by biological processes

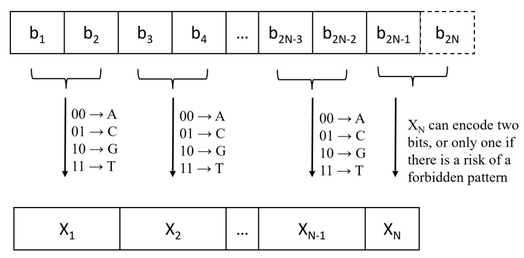
Method

Encoding proposal to ensure data confidentiality

- **Challenge** - Ensure confidentiality under biological constraints while approaching the ideal information rate of 2 bits of information per base
- **Solution** – A three step coding process that includes encryption, dynamic data encoding and error-correction code
  - **Step 1:** Encryption with AES-256 to ensure confidentiality and to regulate the G-C base rate and homopolymers
  - **Step 2:** Dynamic encoding to manage unwanted base patterns; encoding based on the addition or not of one bit of data every *N* bases to avoid homopolymers longer than *N*
  - **Step 3:** Non-binary LDPC error-correction code to correct any base substitutions, deletions or insertions



Encoding solution to ensure data confidentiality in the entire DNA data storage channel

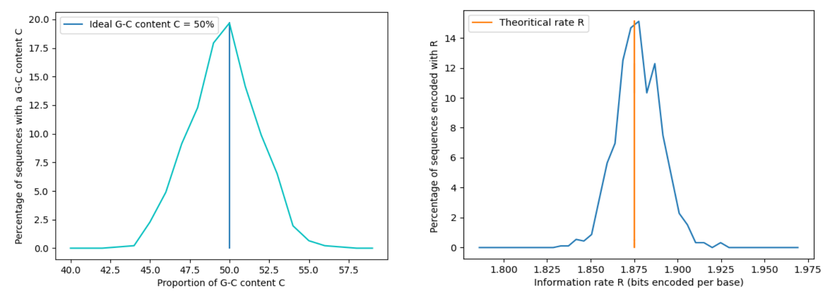


Dynamic encoding of bits into bases. In a block of N bases, each base X_i encodes two bits: b_{2i-1} and b_{2i}, except X_N, which encodes either b_{2N-1} only, or b_{2N-1} and b_{2N}

Simulation and information rate

Experimental results

- **Simulation** of the biological processes using the simulator from [3]
- **Results:** information rate of 1,875 bits per base for *N*=4, no homopolymers longer than *N*, G-C content of 43-57%, data recovery without errors



G-C content (left) and information rate (right) for 1000 sequences of an image after encoding, for N=4 the maximal length of homopolymers authorized

Conclusion and future work

- **Confidentiality** in the entire storage chain that takes into account **biological constraints**
- Encoding solution **independent** from encryption algorithm and error-correction code, **adaptable** to the size of unwanted patterns
- Extend the approach to other synthesis and sequencing technologies

Contact: chloe.berton@imt-atlantique.fr, gouenou.coatrieux@imt-atlantique.fr

References

[1] Rydning, D. R. J. G. J. (2018). The digitization of the world from edge to core. Framingham: International Data Corporation, 16.

[2] De Silva, P. Y., & Ganegoda, G. U. (2016). New trends of digital data storage in DNA. BioMed research international, 2016.

[3] Hamoum, B., Dupraz, E., Conde-Canencia, L., & Lavenier, D. (2021, August). Channel Model with Memory for DNA Data Storage with Nanopore Sequencing. In 2021 11th International Symposium on Topics in Coding (ISTC) (pp. 1-5). IEEE.

March 2022 Colloque de Institut Mines Télécom Palaiseau

Application SPOT de contact-tracing respectueuse de la vie privée

Institut Mines-Télécom

Parties prenantes

TELECOM SudParis

INSTITUT POLYTECHNIQUE DE PARIS

Auteurs

Souha Masmoudi
Nesrine Kaaniche
Maryline Laurent

Partenaires

Institut Mines-Télécom
CHAIRE VALEURS ET POLITIQUES DES INFORMATIONS PERSONNELLES

Protocole sécurisé et respectueux de la vie privée

Une architecture hybride avec plusieurs acteurs

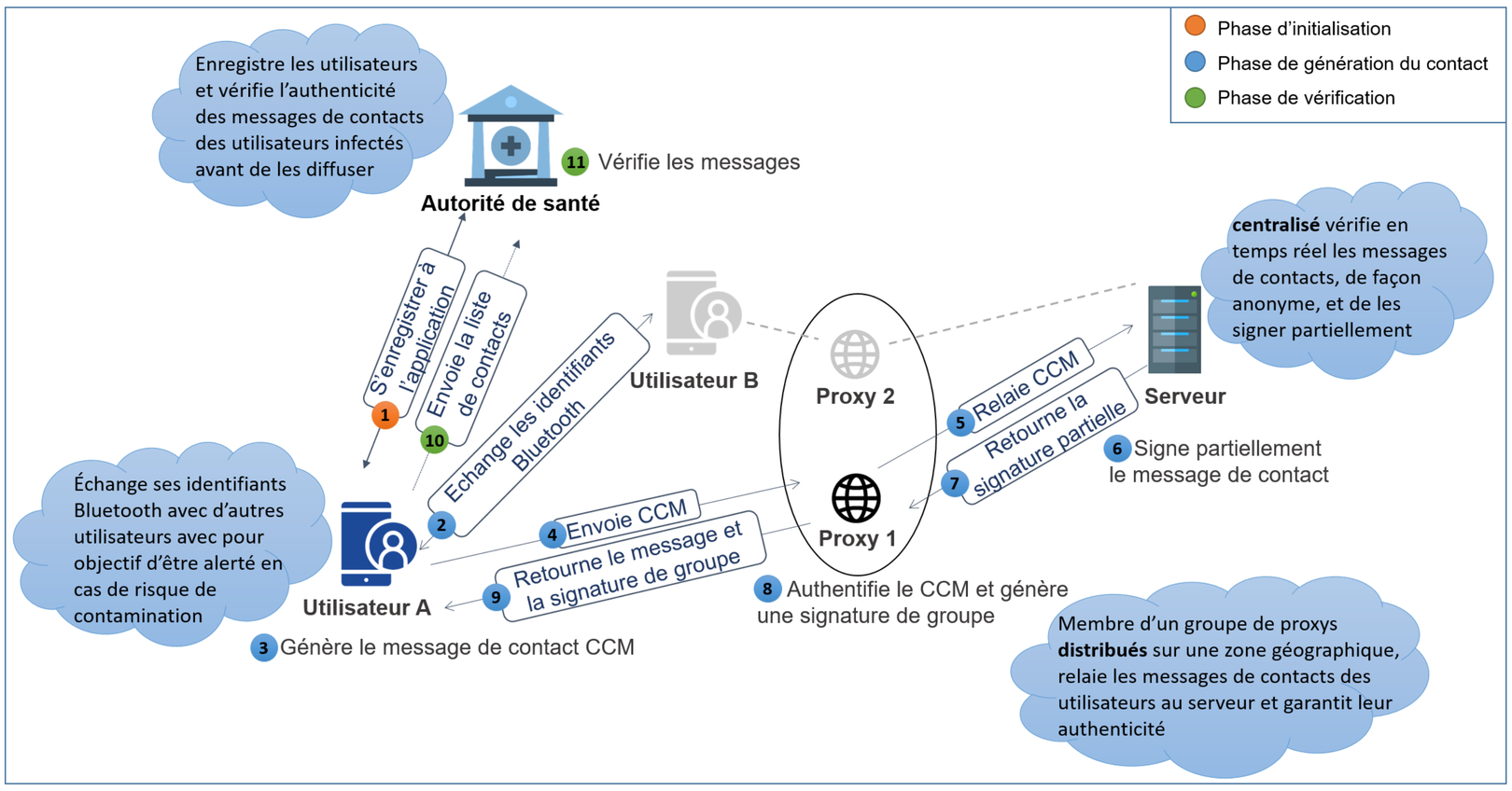


Figure 1 : Architecture et description du protocole SPOT

Un modèle de menaces réaliste et avancé

Des propriétés de sécurité et de respect de la vie privée démontrées

Adversaires	Propriété
	Infalsifiabilité
	Anti-rejeu
	Non-associabilité
	Anonymat

- **Infalsifiabilité** pour empêcher les entités malveillantes de menacer l'authenticité des données
- **Anti-rejeu** pour éviter la soumission des mêmes informations de contact sur différentes sessions
- **Non-associabilité** pour empêcher les entités curieuses d'associer différentes transactions à la même entité
- **Anonymat** pour garantir que des utilisateurs impliqués dans une liste de contacts ne puissent pas être identifiées

Algorithmes de SPOT implémentés, testés et au cœur d'un démonstrateur

Des performances démontrant la faisabilité de la solution

Algorithmes	Entité	Temps d'exécution en ms
Enregistrement à l'application	Autorité de santé / Utilisateur	16 / 31
Génération du CCM	Utilisateur	0,1
Génération de la signature partielle	Serveur	0,02
Génération de la signature de groupe	Proxy	4170
Vérification d'un message de contact	Autorité de santé	37082

Tableau 1 : Temps de calcul des algorithmes de SPOT

- Algorithmes concrets basés sur les signatures de groupes et les preuves à apport nul de connaissance « Non-Interactive Witness-Indistinguishable » (NIWI) de Groth-Sahai
- Algorithmes implémentés utilisant JAVA et testés sur une machine Ubuntu 18.04.3 avec un processeur Intel Core i7 @1.30 GHz et 8 Go de mémoire
- Résultats expérimentaux démontrant l'efficacité et la faisabilité de la solution avec un type de groupe multiplicatif asymétrique et un niveau de sécurité élevé de 128-bits

Contact : souha.masmoudi@telecom-sudparis.eu

Mars 2022 Colloque de l'Institut Mines Télécom Paris