Audition for the position of Associate Professor at LIRMM and Polytech Montpellier

Job n°252414 - Section 61

William Pensec

Post-doctoral researcher,
Laboratoire Hubert Curien,
Université Jean-Monnet,
Saint-Étienne

May 13, 2025

I. Curriculum Vitæ

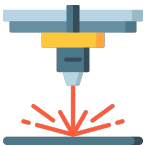
Curriculum Vitæ - General information

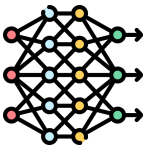
Personal information

- October 1996 (29 years old),
- Post-doctoral researcher,
- CNU qualifications : 61 and 27 (2025).

Research interests

- Hardware Security,
- Physical attacks (Fault Injection Attacks),
- Security of neural network implementations.





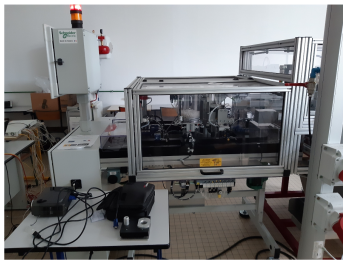
Curriculum Vitæ - Education and Career

- **2019 : Bachelor's degree in Computer Science : Fundamentals and Applications**
  Univ. Bretagne Occidentale - Brest
- **2021 : Master's degree in Computer Science : Software for Embedded Systems**
  Univ. Bretagne Occidentale - Brest - with honours
- **2024 : PhD in Computer Science and Digital Architectures**
  Lab-STICC - Univ. Bretagne Sud - Lorient - European label
- **Now : Post-doctoral researcher**
  Laboratoire Hubert Curien - Univ. Jean Monnet - Saint-Étienne

Curriculum Vitæ - Master 2 Research Internship

Title : Drone cooperation in a heterogeneous environment
Internship Defence : September, 2021 - Brest
Supervisors : David Espès and Catherine Dezan

Objective : Autonomous detection of anomalies on an Industry 4.0 production line using a drone and an embedded neural network.
Publication : 1 peer-reviewed conference with proceedings (ICUAS conference 2022 [1])



1. William Pensec, David Espes et Catherine Dezan. « Smart Anomaly Detection and Monitoring of Industry 4.0 by Drones ». In : *2022 International Conference on Unmanned Aircraft Systems (ICUAS)*. 2022, p. 705-713. DOI : 10.1109/ICUAS54217.2022.9836057

Curriculum Vitæ - PhD Thesis

Title : Enhanced Processor Defence Against Physical and Software Threats by Securing DIFT Against Fault Injection Attacks
PhD Defence : December 19, 2024 - Lorient - European label

Objective : Implementation and evaluation of different lightweight countermeasures to protect a hardware security mechanism (called DIFT) against fault injection attacks.

Composition of the Jury

President of the jury :	Jean-Max Dutertre
Reviewers :	Lejla Batina
	Vincent Beroulle
	Nele Mentens
Examiners :	Francesco Regazzoni
PhD supervisor :	Guy Gogniat
PhD co-supervisor :	Vianney Lapôtre

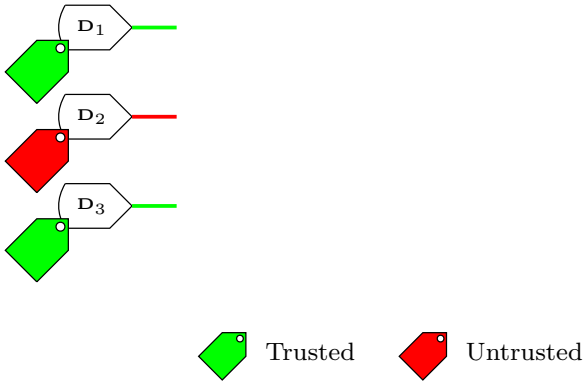
Software threats : Dynamic Information Flow Tracking

- Security mechanism
- Protection against software attacks (e.g. : *buffer overflow*, *format string*, *SQL injections*)
- Follow a security policy
- Associate a tag to each manipulated data

Software threats : Dynamic Information Flow Tracking

Three steps

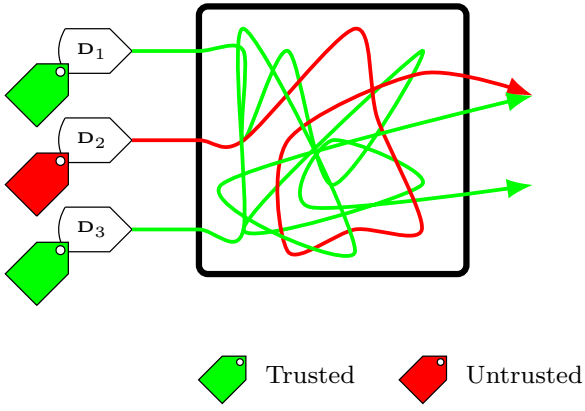
- Tag initialisation
- Tag propagation
- Tag check



Software threats : Dynamic Information Flow Tracking

Three steps

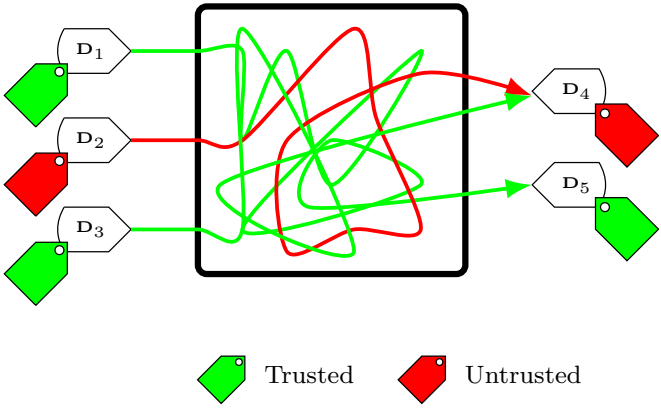
- Tag initialisation
- Tag propagation
- Tag check



Software threats : Dynamic Information Flow Tracking

Three steps

- Tag initialisation
- Tag propagation
- Tag check



D-RI5CY — architecture

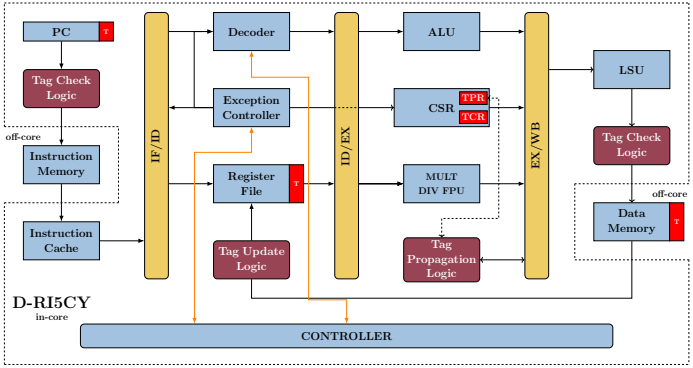


Figure 1 – Architecture of the D-RI5CY.

Security evaluation and overhead

- Use 1-bit tags.
- DIFT induce a 5% overhead on the area.
- No impact on the processor performance.
- Tested against different use cases of software attacks (buffer overflow, format string).
- No false positive.

Curriculum Vitæ - Publications

- Overview of all my publications

	Total
Conferences with proceedings	5
Invited talks	6
Posters	8

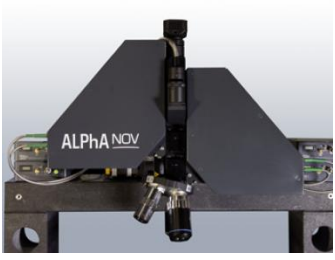
- Award
  - Best paper award at Sensors S&P 2023
- International collaborations
  - Research visit at Università della Svizerra italiana (Lugano) for 5 months in 2023 with Francesco Regazzoni (led to the publication of 1 conference paper [2] and to the submission of 1 journal paper)

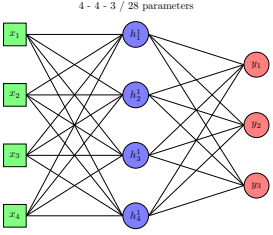
2. William PENSEC et al. « Defending the Citadel : Fault Injection Attacks Against Dynamic Information Flow Tracking and Related Countermeasures ». In : *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. Knoxville, United States, juill. 2024, p. 180-185. DOI : 10.1109/ISVLSI61997.2024.00042

Title : Security Evaluation of Neural Network implementations against Fault Injection Attacks

Collaboration with : Vincent Grosso, Brice Colombier, Cédric Killian

Objective : Cloning a trained model on a dataset (MNIST, Iris, ...) thanks to fault injections in the flash memory to recover the weights of the original model.





II. Projet d'intégration en enseignement à Polytech Montpellier

Polytech Montpellier

- École appartenant au réseau des 16 écoles Polytech en France
- $\approx$ 1400 étudiants / $\approx$ 300 diplômés par an
- Cycle préparatoire aux écoles Polytech (après concours Geipi) : 2 ans
- 10 formations au cycle d'ingénieur (FISA et FISE) : 3 ans
- 2 formations dans le département Électronique et Informatique Industrielle (parcours Microélectronique et Automatique (FISE) et parcours Systèmes Embarqués (FISA))

POLYTECH MONTPELLIER

L'AVENIR DEPUIS 1220 UNIVERSITÉ DE MONTPELLIER

Projet d'intégration : Enseignements dispensés

- Aperçu de mes enseignements, par année d'étude

Année d'étude	Type	Nombre d'heures
BUT 1	TD/TP	48
BUT 2	TP	64
Master 1 / FISE 2	Projet	23
Master 2	TP	8
TOTAL		143

- Cadre de mes enseignements
  - IUT de Lorient (département GIM)
  - Faculté des Sciences de Lorient (Masters SESI (Systèmes Embarqués et Systèmes Intégrés) et CSSE (Cyber-Sécurité des Systèmes Embarqués))
  - Télécom Saint-Étienne

Projet d'intégration : Enseignements en programmation

- Cours suivis : programmation impérative (C), objet (C++, Java), web, parallèle (OpenMP, notions de CUDA)
- Cours donnés : programmation C, Python, introduction à la programmation parallèle (OpenMP)

- Cours visés : programmation impérative, objet, Linux, shell, BDD, cours d'informatique au sein du cycle préparatoire PeiP (parcours A)

Promotion	**Nom de l'UE**	**Type**	**Effectif**	**Nombre d'heures**
BUT GIM 2	INFO (programmation C)	TP	12–14	44
BUT GIM 2	INFO (programmation python)	TP	12–14	20
Master 2	Introduction à la progammation parallèle	TP	13	8
			TOTAL	72

Projet d'intégration : Enseignements en systèmes embarqués

- Cours suivis : IA embarqué, OS embarqués et temps réel, ordonnancement de tâches, sûreté de fonctionnement
- Cours donné : Encadrement de projet industriel en tant qu'encadrant universitaire

- Cours visés : Informatique embarquée, systèmes, OS temps réel et architecture

Promotion	**Nom de l'UE**	**Type**	**Effectif**	**Nombre d'heures**
FISE 2	Projets Industriels (PING)	Projet	4	7
			TOTAL	7

Projet d'intégration : Enseignements en électronique

- Cours suivis : synthèse co-design, SoC
- Cours donnés : Conception d'Architecture Numérique, électronique numérique, logique booléenne

- Cours visés : électronique numérique, microcontrôleurs, logique et VHDL

Promotion	**Nom de l'UE**	**Type**	**Effectif**	**Nombre d'heures**
BUT GIM 1	Introduction à l'électronique numérique et à la logique booléenne	TD	12	8
BUT GIM 1	Introduction à l'électronique numérique et à la logique booléenne	TP	12–14	40
Master 1	Conception d'Architecture Numérique	TP/Projet	15	16
			TOTAL	64

Projet d'intégration : Enseignements à Polytech

Enseignements réalisables immédiatement (non exhaustif)

- Programmation informatique (langage C, algorithmique) et objet (UE XASE502 / XA9S711B)
- Électronique (UE XASE622)
- Bases de données (UE XASE614)
- Introduction à la programmation réseau (UE XASE911 / XA9S516A)
- Introduction à Linux / shell (UE XASE514 / XASE820A)
- Systèmes, OS temps réel et architecture (UE XASE721A)

Enseignements à moyen terme (non exhaustif)

Ordonnancement / Logique et VHDL / Cryptographie et sécurité

Projet d'intégration : Responsabilités administratives

Motivations pour prendre des responsabilités

- Gestion d'une année d'étude
- Organisation des stages
- Admission des étudiants à l'école

III. Projet d'intégration en recherche au LIRMM

Intégration au laboratoire

Thèmes de recherche

- Sécurité matérielle des systèmes embarqués / processeurs RISC-V,
- Attaques physiques (plus spécifiquement : attaques par injections de fautes),
- Sécurité des implémentations de réseaux de neurones contre les attaques par injections de fautes.

LIRMM

- Équipe ADAC : travaille sur les notions de sécurité des systèmes embarqués, la conception d'architectures matérielles, ainsi que l'Internet des Objets (IoT).
- Équipe SmartIES : travaille à la conception et l'analyse de systèmes intégrés avec comme objectifs principaux la sécurité matérielle contre les attaques physiques, ainsi que l'efficacité énergétique.
- Équipe TEST : travaille sur le test, la fiabilité et la sécurité des circuits intégrés, notamment contre les attaques physiques, ainsi qu'en environnement radiatif et spatial.

Contexte de ma recherche : l'IoT menacé

Menaces

- Menaces réseaux : Man-In-The-Middle [3], jamming [4], déni de service
- **Menaces logicielles** : attaques par débordement de mémoire [5], exécution de code, injections SQL
- **Menaces matérielles** : rétro-ingénierie, attaques par canal auxiliaire [6], injection de fautes (FIA) [7]

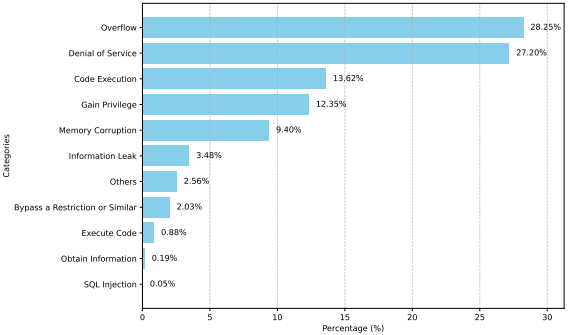


Figure 2 – Données de BitDefender [8]

Thème de recherche - Objectifs

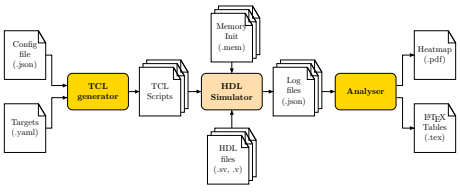
Problématique

Comment évaluer et maintenir une sécurité maximale des systèmes embarqués en présence d'attaques physiques ?

Contribution : Simulation d'Injection de Fautes pour l'Évaluation de la Sécurité (FISSA)

FISSA

- Outil open-source disponible sur GitHub [9] présenté à DSD 2024 [10]
- Permet au concepteur de circuit d'analyser tout au long du cycle de conception la sensibilité contre les FIA.
- Il est intégré à un simulateur HDL (Questasim).
- Les résultats générés peuvent aider à trouver des vulnérabilités pendant la phase de conception.
- FISSA met en œuvre les principes de la sécurité par la conception.



Contre-mesures implémentées

- Proposition de 5 stratégies d'implémentations de contre-mesures légères basées sur les codes de parités.
- Surcoût de surface inférieur à 8% (sur un petit processeur).
- Aucun impact sur les performances.
- Très bon résultats en termes de sécurité :
  - 100% de détection/correction des attaques sur des modèles de fautes simples (jusqu'à 2 fautes injectées) ;
  - 99.99% de détection/correction des attaques sur des modèles de fautes complexes (jusqu'à 11 fautes injectées).

Second thème de recherche - Objectif

Problématique

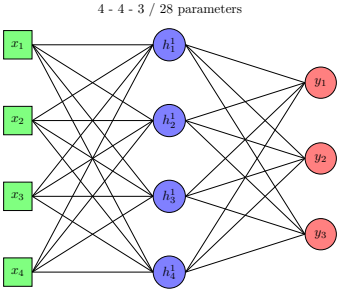
- Comment obtenir par rétro-ingénierie un modèle équivalent à un réseau de neurones entraîné en ayant accès seulement aux entrées et aux valeurs de sorties ?

Expérimentations

- Injection de fautes lasers dans la mémoire flash (bit set seulement) afin de modifier le signe des poids.
- Confirmation du fonctionnement de l'algorithme en simulations avant expérimentations réelles sur banc laser.

Résultats préliminaires

- Travaux en cours - débuté en octobre dernier
- Clonage réussi sur des petits modèles aléatoires ainsi que sur des modèles entraînés avec le dataset *iris*.
- Modèles à 3 couches pour le moment seulement.
- Plus gros modèles à tester et sur d'autres dataset.



Évaluation de la sécurité

- Identification de vulnérabilités microarchitecturales (notion de *Sécurité à la Conception*) :
  - ISA RISC-V.
  - Projet ANR SCAMA (équipe ADAC) sur la création d'un processeur sécurisé à la conception contre les attaques microarchitecturales.
  - Projet ANR SCREAM sur la proposition d'une architecture de processeur RISC-V intégrant des composants non-volatiles à base de cellules MRAM.
- Continuer le développement de FISSA :
  - intégration d'autres simulateurs (exemples : Vivado, Verilator),
  - ajout d'autres modèles de fautes plus spécifiques ou selon l'état de l'art
- Expérimenter sur bancs réels pour confirmer ces vulnérabilités :
  - attaques par canaux cachés,
  - attaques par injection de fautes.

Protection des systèmes

- Proposer des protections efficaces et légères :
  - redondance (matérielle, temporelle),
  - rejeu,
  - obfuscation,
  - codes de parités (redondance d'information)
    - Simple parité
    - Hamming Code
    - Hamming Code - SECDED

Conclusion des projets d'intégration

Enseignements

- ✓ Enseignements opérationnels : langages de programmation, électronique, systèmes embarqués
- ✓ Enseignements à moyen termes : ordonnancement, cryptographie, VHDL
- ✓ Motivé par la prise de responsabilités administratives (gestion d'une année, organisation de stages, etc)

Conclusion des projets d'intégration

Équipes

- Travaux en commun avec les équipes ADAC et/ou SmartIES sur les aspects de sécurité des systèmes embarqués.
- Collaborations avec l'équipe TEST, travaillant sur les notions de test, de fiabilité et de sécurité des systèmes embarqués, ainsi que sur les notions d'environnement radiatif.

Ce que je propose

- Étude de vulnérabilités en simulation ainsi qu'en expérimentation sur banc d'essai contre les attaques physiques (canaux auxiliaires ou injections de fautes).
- Développement de l'outil FISSA selon les progrès de l'état de l'art.
- Étude et proposition de protections ciblant des systèmes embarqués légers contre les vulnérabilités trouvées $\Rightarrow$ compétences dans les codes de parités et théorie de l'information.

Audition for the position of Associate Professor at LIRMM and Polytech Montpellier

Job n°252414 - Section 61

William Pensec

Post-doctoral researcher,
Laboratoire Hubert Curien,
Université Jean-Monnet,
Saint-Étienne

Merci pour votre attention.

Bibliographie

References

[1] William Pensec, David Espes et Catherine Dezan. « Smart Anomaly Detection and Monitoring of Industry 4.0 by Drones ». In : *2022 International Conference on Unmanned Aircraft Systems (ICUAS)*. 2022, p. 705-713. doi : 10.1109/ICUAS54217.2022.9836057.

[2] William PENSEC et al. « Defending the Citadel : Fault Injection Attacks Against Dynamic Information Flow Tracking and Related Countermeasures ». In : *2024 IEEE Computer Society Annual Symposium on VLSI (ISVLSI)*. Knoxville, United States, juill. 2024, p. 180-185. doi : 10.1109/ISVLSI61997.2024.00042.

[3] Mauro Conti, Nicola Dragoni et Viktor Lesyk. « A Survey of Man In The Middle Attacks ». In : *IEEE Communications Surveys & Tutorials* 18.3 (2016), p. 2027-2051. doi : 10.1109/COMST.2016.2548426.

[4] Hossein Pirayesh et Huacheng Zeng. « Jamming Attacks and Anti-Jamming Strategies in Wireless Networks : A Comprehensive Survey ». In : *IEEE Communications Surveys & Tutorials* 24.2 (2022), p. 767-809. doi : 10.1109/COMST.2022.3159185.

[5] C. Cowan et al. « Buffer overflows : attacks and defenses for the vulnerability of the decade ». In : *Proceedings DARPA Information Survivability Conference and Exposition. DISCEX'00*. T. 2. 2000, 119-129 vol.2. doi : 10.1109/DISCEX.2000.821514.

[6] Mampi Devi et Abhishek Majumder. « Side-Channel Attack in Internet of Things : A Survey ». In : *Applications of Internet of Things*. Singapore : Springer Singapore, 2021, p. 213-222. isbn : 978-981-15-6198-6. doi : 10.1007/978-981-15-6198-6_20.

[7] H. Bar-El et al. « The Sorcerer's Apprentice Guide to Fault Attacks ». In : *Proceedings of the IEEE* 94.2 (2006), p. 370-382. doi : 10.1109/JPROC.2005.862424.

References

[8] *The 2024 IoT Security Landscape Report*. 2024. URL : https://blogapp.bitdefender.com/hotforsecurity/content/files/2024/06/2024-IoT-Security-Landscape-Report_consumer.pdf.

[9] William Pensec. *FISSA : Fault Injection Simulation for Security Assessment*. URL : https://github.com/WilliamPsc/FISSA.

[10] William Pensec, Vianney Lapôtre et Guy Gogniat. « Scripting the Unpredictable : Automate Fault Injection in RTL Simulation for Vulnerability Assessment ». In : *2024 27th Euromicro Conference on Digital System Design (DSD)*. Paris, France, août 2024, p. 369-376. DOI : 10.1109/DSD64264.2024.00056.

[11] Freepik Company. *Icônes vectorielles*. 2010. URL : https://www.flaticon.com/.

[12] R. W. Hamming. « Error detecting and error correcting codes ». In : *The Bell System Technical Journal* (1950). DOI : 10.1002/j.1538-7305.1950.tb00463.x.

Questions

Code de Hamming

- Codes correcteurs d'erreurs linéaires, inventés par Richard W. Hamming [12].
- Principalement utilisés dans les systèmes de communication numérique et de stockage de données.
- Détectent et corrigent les erreurs sur un seul bit.
- Les bits de redondance sont placés dans des positions de puissance de 2.

$$
\begin{aligned}
r_0 &= d_0 \oplus d_1 \oplus d_3 \oplus d_4 \oplus d_6 \\
r_1 &= d_0 \oplus d_2 \oplus d_3 \oplus d_5 \oplus d_6 \\
r_2 &= d_1 \oplus d_2 \oplus d_3 \\
r_3 &= d_4 \oplus d_5 \oplus d_6
\end{aligned}
\tag{1}
$$

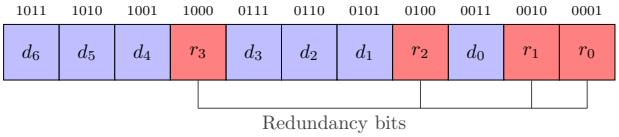


Figure 3 – Hamming codeword

Code de Hamming - SECDED

- Basé sur le code de Hamming.
- Détecte les erreurs sur deux bits et corrige les erreurs sur un seul bit.
- Un bit supplémentaire est ajouté : le bit de parité général.

$$
\begin{aligned}
r_0 &= d_0 \oplus d_1 \oplus d_3 \oplus d_4 \oplus d_6 \\
r_1 &= d_0 \oplus d_2 \oplus d_3 \oplus d_5 \oplus d_6 \\
r_2 &= d_1 \oplus d_2 \oplus d_3 \\
r_3 &= d_4 \oplus d_5 \oplus d_6 \\
gp_0 &= \bigoplus_{i=0}^{6} d_i \oplus \bigoplus_{j=0}^{3} r_j
\end{aligned}
\tag{2}
$$

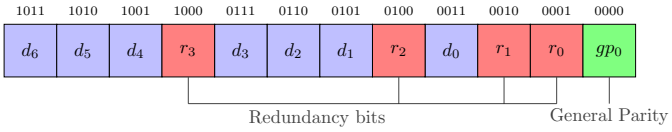


Figure 4 – SECDED codeword