Clémentine MAURICE

Chargée de Recherche CNRS

Campus de Beaulieu, 263 avenue du Général Leclerc
35042 RENNES cedex
✉ *clementine.maurice@irisa.fr*
cmaurice.fr

Thématiques de recherche

Mes travaux et mon projet de recherche portent sur la **sécurité** et la protection de la vie privée, du point de vue des systèmes d'information, et plus précisément dans l'**interaction entre le logiciel et le matériel**. Mes travaux de recherche s'attachent à analyser les fuites d'informations sensibles dues à la **micro-architecture des processeurs** et les attaques par fautes ne requérant aucun accès matériel. Ma recherche a pour but de créer des contre-mesures à ces attaques qui soient à la fois robustes, performantes, et adaptées aux appareils du quotidien tels que les appareils mobiles, les ordinateurs portables et personnels ainsi que les serveurs dans les environnements de type cloud computing. Une première étape nécessaire est la recherche des vecteurs d'attaques ainsi que l'évaluation du réalisme de ces attaques. Ces attaques exploitant des composants très complexes et souvent non documentés, un de mes axes de recherche consiste également en la rétro-ingénierie de ces composants matériels.

Curriculum Vitae

depuis 2017 **Chargée de Recherche CNRS**, *équipe EMSEC, IRISA*, Rennes.

2016–2017 **Chercheuse postdoctorale**, *équipe Secure Systems, IAIK, TU Graz*, Autriche.

2012–2015 **Doctorante**, *CIFRE Eurecom/Technicolor*, Sophia Antipolis et Cesson-Sévigné.
Thèse de doctorat: Fuites d'information dans les processeurs récents et applications à la virtualisation.
- Juin 2015 : visite de deux semaines dans l'équipe Secure Systems de TU Graz en Autriche pour travailler sur la première attaque par faute logicielle depuis un navigateur en JavaScript [15].

2007-2012 **Élève-ingénieur**, *INSA*, Rennes, France.
Double diplôme : Diplôme d'Ingénieur et Master Recherche en Informatique.
Parcours : Sécurité des systèmes d'information.
- 2012 : Stage de recherche en industrie (6 mois) à Technicolor, laboratoire Security & content protection, Cesson-Sévigné, France. Amélioration des techniques de fingerprinting 802.11.
- 2011 : Stage de recherche (2 mois) à Inria, équipe Texmex, Rennes, France. Segmentation thématique de documents télévisuels.

Publications

Les conférences reconnues par les pairs comme étant les meilleures dans le domaine de la sécurité informatique sont ACM CCS, IEEE S&P, Usenix Security et NDSS. J'ai publié six articles dans trois de ces conférences de renom. Le taux d'acceptation est donné pour chaque conférence, quand il est connu. Dans mon domaine, il est d'usage que les auteurs soient ordonnés par rapport à leurs contributions respectives. Ma visibilité est reflétée par mon h-index de 17 ainsi que mes 2270 citations (selon Google Scholar en septembre 2020).

Revues internationales avec comité de lecture

[1] Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, and Stefan Mangard. "Malware Guard Extension: Abusing Intel SGX to conceal cache attacks". In: *Cybersecurity* 3 (Jan. 2020).

[2] Sarani Bhattacharya, Clémentine Maurice, Shivam Bhasin, and Debdeep Mukhopadhyay. "Branch Prediction Attack on Blinded Scalar Multiplication". In: *IEEE Transactions on Computers* 69.5 (2020), pp. 633–648.

Conférences internationales avec comité de lecture

[3] Moritz Lipp, Vedad Hadžić, Michael Schwarz, Arthur Perais, Clémentine Maurice, and Daniel Gruss. "Take A Way: Exploring the Security Implications of AMD's Cache Way Predictors". In: *Proceedings of the 15th ACM ASIA Conference on Computer and Communications Security (ASIACCS'20)*. ASIACCS. Taux d'acceptation : 21.8%. ACM, June 2020.

[4] Michael Schwarz, Daniel Gruss, Moritz Lipp, Clémentine Maurice, Thomas Schuster, Anders Fogh, and Stefan Mangard. "Automated Detection, Exploitation, and Elimination of Double-Fetch Bugs using Modern CPU Features". In: *Proceedings of the 13th ACM Asia Conference on Computer and Communications Security*. ASIACCS. Taux d'acceptation : 20.0%. ACM, May 2018.

[5] Michael Schwarz, Moritz Lipp, Daniel Gruss, Samuel Weiser, Clémentine Maurice, Raphael Spreitzer, and Stefan Mangard. "KeyDrown: Eliminating Software-Based Keystroke Timing Side-Channel Attacks". In: *Proceedings of the 25th Annual Network and Distributed System Security Symposium*. NDSS. Taux d'acceptation : 21.5%. The Internet Society, Feb. 2018.

[6] Moritz Lipp, Daniel Gruss, Michael Schwarz, David Bidner, Clémentine Maurice, and Stefan Mangard. "Practical Keystroke Timing Attacks in Sandboxed JavaScript". In: *Proceedings of the 22nd European Symposium on Research in Computer Security*. ESORICS. Taux d'acceptation : 15.9%. Springer, Sept. 2017.

[7] Daniel Gruss, Moritz Lipp, Michael Schwarz, Richard Fellner, Clémentine Maurice, and Stefan Mangard. "KASLR is Dead: Long Live KASLR". In: *Proceedings of the 9th International Symposium on Engineering Secure Software and Systems*. ESSoS. Taux d'acceptation : 46.9%. Springer, July 2017.

[8] Michael Schwarz, Samuel Weiser, Daniel Gruss, Clémentine Maurice, and Stefan Mangard. "Malware Guard Extension: Using SGX to Conceal Cache Attacks". In: *Proceedings of the 14th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*. DIMVA. Taux d'acceptation : 26.9%. Springer, July 2017.

[9] Michael Schwarz, Clémentine Maurice, Daniel Gruss, and Stefan Mangard. "Fantastic Timers and Where to Find Them: High-Resolution Microarchitectural Attacks in JavaScript". In: *Proceedings of the 21st International Conference on Financial Cryptography and Data Security*. FC. Springer, Apr. 2017.

[10] Clémentine Maurice, Manuel Weber, Michael Schwarz, Lukas Giner, Daniel Gruss, Carlo Alberto Boano, Stefan Mangard, and Kay Römer. "Hello from the Other Side: SSH over Robust Cache Covert Channels in the Cloud". In: *Proceedings of the 24th Annual Network and Distributed System Security Symposium*. NDSS. Taux d'acceptation : 16.1%. The Internet Society, Feb. 2017.

[11] Daniel Gruss, Clémentine Maurice, Anders Fogh, Moritz Lipp, and Stefan Mangard. "Prefetch Side-Channel Attacks: Bypassing SMAP and Kernel ASLR". In: *Proceedings of the 23rd ACM Conference on Computer and Communications Security*. CCS. Taux d'acceptation : 16.4%. ACM, Nov. 2016.

[12] Victor van der Veen, Yanick Fratantonio, Martina Lindorfer, Daniel Gruss, Clémentine Maurice, Giovanni Vigna, Herbert Bos, Kaveh Razavi, and Cristiano Giuffrida. "Drammer: Deterministic Rowhammer Attacks on Mobile Platforms". In: *Proceedings of the 23rd ACM Conference on Computer and Communications Security*. CCS. Taux d'acceptation : 16.4%. ACM, Nov. 2016.

[13] Moritz Lipp, Daniel Gruss, Raphael Spreitzer, Clémentine Maurice, and Stefan Mangard. "ARMageddon: Cache Attacks on Mobile Devices". In: *Proceedings of the 25th USENIX Security Symposium*. USENIX Security. Taux d'acceptation : 15.6%. USENIX Association, Aug. 2016, pp. 549–564.

[14] Peter Pessl, Daniel Gruss, Clémentine Maurice, Michael Schwarz, and Stefan Mangard. "DRAMA: Exploiting DRAM Addressing for Cross-CPU Attacks". In: *Proceedings of the 25th USENIX Security Symposium*. USENIX Security. Taux d'acceptation : 15.6%. USENIX Association, Aug. 2016, pp. 565–581.

[15] Daniel Gruss, Clémentine Maurice, and Stefan Mangard. "Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript". In: *Proceedings of the 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*. DIMVA. Taux d'acceptation : 31.8%. Springer, July 2016, pp. 300–321.

[16] Daniel Gruss, Clémentine Maurice, Klaus Wagner, and Stefan Mangard. "Flush+Flush: A Fast and Stealthy Cache Attack". In: *Proceedings of the 13th Conference on Detection of Intrusions and Malware & Vulnerability Assessment*. DIMVA. Taux d'acceptation : 31.8%. Springer, July 2016, pp. 279–299.

[17] Clémentine Maurice, Nicolas Le Scouarnec, Christoph Neumann, Olivier Heen, and Aurélien Francillon. "Reverse Engineering Intel Last-Level Cache Complex Addressing Using Performance Counters". In: *Proceedings of the 18th International Symposium on Research in Attacks, Intrusions and Defenses*. RAID. Taux d'acceptation : 23.5%. Springer, Nov. 2015, pp. 48–65.

[18] Clémentine Maurice, Christoph Neumann, Olivier Heen, and Aurélien Francillon. "C5: Cross-Cores Cache Covert Channel". In: *Proceedings of the 12th Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. DIMVA. Taux d'acceptation : 22.7%. Springer, July 2015, pp. 46–64.

[19] Clémentine Maurice, Christoph Neumann, Olivier Heen, and Aurélien Francillon. "Confidentiality Issues on a GPU in a Virtualized Environment". In: *Proceedings of the 18th International Conference on Financial Cryptography and Data Security*. FC. Taux d'acceptation : 22.5%. Springer, Mar. 2014, pp. 119–135.

[20] Clémentine Maurice, Stéphane Onno, Christoph Neumann, Olivier Heen, and Aurélien Francillon. "Improving 802.11 Fingerprinting of Similar Devices by Cooperative Fingerprinting". In: *Proceedings of the 2013 International Conference on Security and Cryptography*. SECRYPT. Springer, Aug. 2013, pp. 379–386.

Workshops internationaux avec comité de lecture

[21] Moritz Lipp, Misiker Tadesse Aga, Michael Schwarz, Daniel Gruss, Clémentine Maurice, Lukas Raab, and Lukas Lamster. "Nethammer: Inducing Rowhammer Faults through Network Requests". In: *Proceedings of the 2020 Workshop on the Security of Software / Hardware Interfaces (SILM)*. co-localisé avec EuroS&P. June 2020.

Articles de vulgarisation

[22] Clémentine Maurice. "Meltdown et attaques sur KASLR : les attaques par canal auxiliaire passent à la vitesse supérieure". In: *MISC n°97* (May 2018).

[23] Clémentine Maurice. "Après Meltdown et Spectre, comment sécuriser les processeurs ?" In: *Le Journal du CNRS* (Mar. 2018).

Brevets

[24] Clémentine Maurice, Olivier Heen, Christoph Neumann, and Aurélien Francillon. *Method and apparatus for cross-core covert channel*. US Patent 20,160,117,246. Apr. 2016.

[25] Christoph Neumann, Olivier Heen, and Clémentine Maurice. *Device and method for record linkage*. European Patent Application EP 3 093 776 A1. Nov. 2016.

[26] Christoph Neumann, Olivier Heen, Clémentine Maurice, and Stéphane Onno. *Method and device for countering fingerprint forgery attacks in a communication system*. US Patent 9,143,528. Sept. 2015.

Service académique et responsabilités administratives

Membre de comité de pilotage de conférences et de workshops
- Workshop on Offensive Technologies (WOOT) depuis 2020

Responsable de comité de programme de conférences et de workshops — le classement Core est donné quand il est connu (`http://portal.core.edu.au/conf-ranks`)
- USENIX Security Symposium 2021, rang A*, **artifact evaluation committee co-chair**
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2020, rang C, **PC chair**
- Workshop on Offensive Technologies (WOOT) 2019 (co-localisé avec Usenix Security), **PC co-chair**
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2019, rang C, **PC co-chair**

Membre de comité de programme de conférences internationales — le classement Core est donné quand il est connu (`http://portal.core.edu.au/conf-ranks`)
- IEEE Symposium on Security and Privacy (**S&P**) 2021, rang A*
- USENIX Security Symposium (**USENIX Sec**) 2020, rang A*
- IEEE Symposium on Security and Privacy (**S&P**) 2020, rang A*
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2018, rang C
- International Conference on Distributed Computing Systems (**ICDCS**) 2018, Security track, rang A
- World Wide Web Conference (**WWW**) 2018, Security and Privacy research track, rang A*
- Conference on Cryptographic Hardware and Embedded Systems (**CHES**) 2018, rang A
- Annual Computer Security Applications Conference (**ACSAC**) 2017, rang A
- International Symposium on Engineering Secure Software and Systems (ESSoS) 2017

Membre de comité de programme de workshops internationaux et de conférences nationales
- Symposium sur la sécurité des technologies de l'information et des communications (SSTIC) 2020
- Symposium sur la sécurité des technologies de l'information et des communications (SSTIC) 2019
- European Workshop on Systems Security (EuroSec) 2019
- Reversing and Offensive-oriented Trends Symposium (ROOTS) 2018
- Workshop on Offensive Technologies (WOOT) 2018 (co-localisé avec Usenix Security)
- Symposium sur la sécurité des technologies de l'information et des communications (SSTIC) 2018

Relectrice pour des revues internationales à comité de lecture
- Journal of Computer Security, 2019
- ACM Transactions on Embedded Computing Systems, 2019
- IEEE Transactions on Emerging Topics in Computing (TETC), 2017
- Elsevier Microprocessors and Microsystems (MICPRO), 2017
- ACM Transactions on Internet Technology (TOIT), 2016
- IEEE Transactions on Information Forensics & Security (T-IFS), 2014

Relectrice externe : SAC 2019, CCS 2017, VLSI-SoC 2017, DIMVA 2017, RAID 2017, AsiaCCS 2017, DATE 2017, NDSS 2017, ACSAC 2016, ICDCS 2016, WOOT 2015, Eurosec 2013, ESORICS 2013

Membre de comité de sélection et de prix
- Secrétaire du prix de thèse Gilles Kahn de la Société Informatique de France (SIF), 2019, 2020
- Membre du jury de prix de thèse Gilles Kahn de la Société Informatique de France (SIF), 2018

- Membre du comité de sélection de Maître de Conférences à l'INSA de Toulouse, 2018

Jurys de thèses
- Nampoina Andriamilanto, "Authentification Forte par Browser Fingerprinting", Université de Rennes, France, TBD
- Sébastien Carré, "Attaques exploitant le temps de calcul : modélisation et protections", Télécom Paris, France, Décembre 2020
- Radhesh Konoth, "Vulnerable by Design: Mitigating Design Flaws in Hardware and Software", VU Amsterdam, Pays-Bas, Décembre 2020
- Pepe Vila, "Learning Secrets and Models from Execution Time", IMDEA Software Institute, Espagne, Juin 2020
- Antoine Vastel, "Tracking Versus Security: Investigating the Two Facets of Browser Fingerprinting", Université de Lille, France, Octobre 2019
- Fabio Pagani, "Advances in memory forensics", EURECOM, France, Septembre 2019

Organisation d'événements
- Organisation de l'école d'été du GDR Sécurité, 2019, Rennes, France
- Publicité pour l'école de printemps Security & Correctness in the IoT 2017, Graz, Autriche
- Organisation sur site pour COSADE 2016, Graz, Autriche

Responsabilités administratives
- Membre de la commission électorale du conseil de laboratoire de l'IRISA, 2018

Supervision d'étudiants

Doctorants
- Pierre Ayoub, 2020-2023
- Thomas Rokicki, 2019-2022
- Guillaume Didier, 2019-2022
- Christophe Genevey-Metat, 2018-2021

Postdocs
- Sam Thomas, 2018-2019

Étudiants de master
Léo Cosseron (2020), Pierre Ayoub (2020), Julius Wenzel (2020), Thibaut Perami (2019), Thomas Rokicki (2019), Lukas Giner (2016).

Projets

2019–2023 **ANR JCJC** MIAOUS (porteuse du projet)
2019–2023 ANR ARCHI-SEC (responsable scientifique IRISA)
2019–2023 ANR MobiS5 (membre)
2018 Financement PEPS JCJC INS2I de 8,000€ pour démarrer mon activité de recherche à l'IRISA.
2018–2020 Financement DGA de 158 400€ pour le recrutement d'un chercheur postdoctoral pour 2 ans.

Prix

2018 **Prix Bretagne Jeune Chercheuse et Chercheur** dans la catégorie "Technologies de Pointe".
2015 **Best Paper Award** à la conférence DIMVA pour l'article [18].

Diffusion scientifique

J'ai présenté mes travaux de recherche dans des **séminaires d'équipes** internationales à l'occasion de visites, comme à Vienne ou à Bochum, ainsi que dans des **écoles de jeunes chercheurs**. Par ailleurs, deux **industriels** majeurs du domaine des micro-processeurs, à savoir Intel et Qualcomm, m'ont également invité à présenter mes travaux. Enfin, j'ai présenté mes travaux à des **conférences non académiques**, comme le Chaos Communication Congress, BlackHat Europe, ou les Rencontres Mondiales du Logiciel Libre. En effet, la communauté de sécurité organise beaucoup de conférences où les chercheurs académiques, industriels, ou plus généralement les passionnés peuvent se rencontrer. L'audience y est à la fois très large (12 000 personnes au Chaos Communication Congress de Hambourg) et également très diverse.
La liste complète de mes présentations est disponible sur ma page web: `https://cmaurice.fr`

2020 Masterclass au Forum International de la Cybersécurité (FIC), Lille, France

2019 Présentation invitée à la conférence FICHSA, Tel Aviv, Israel
Cours invité à Ben-Gurion University of the Negev, Beer Sheva, Israel
Présentation invitée à la journée sécurité, INSA Toulouse, France

2018 Présentation invitée au 8th Inria/Technicolor Workshop On Systems (WOS8), Rennes, France
Présentation invitée au Séminaire du DIT, ENS Rennes, France
Cours invité (Skype) au Indian Institute of Technology Kanpur, Inde
Présentation invitée au Séminaire Sécurité du LORIA, Nancy, France
Travaux pratiques à l'école d'été Cyber in Occitanie, Montpellier, France
Présentation invitée au Colloque Architecture, Toulouse, France
Présentation invitée aux journées nationales pré-GDR Sécurité Informatique, Paris, France

2017 Présentation aux RMLL 2017, Saint-Étienne, France
Présentation invitée au SSTIC 2017, Rennes, France
Cours à l'école de printemps Security & Correctness in the IoT, Graz, Autriche
Présentation à RuhrSec 2017, Bochum, Allemagne
Keynote à XDOM0 2017 (workshop co-localisé avec EuroSys), Belgrade, Serbie
Présentations invitées à Intel, Hillsboro, Oregon, USA
Présentation invitée à Qualcomm, San Diego, Californie, USA

2016 Présentation au Chaos Communication Congress (33C3), Hambourg, Allemagne
Présentation invitée à SBA Research, Vienne, Autriche
Cours invité au HackerPraktikum, Ruhr-University Bochum, Allemagne
Présentation invitée à Ruhr-University Bochum, Allemagne
Présentation à BlackHat Europe 2016, Londres, UK
Cours invité à l'école d'été IPICS 2016 à KU Leuven, Belgique

2015 Présentation au Chaos Communication Congress (32C3), Hambourg, Allemagne
Présentation invitée au séminaire d'équipe Secure Systems, IAIK, TU Graz, Autriche

2013 Présentation au 3rd Workshop on Storage and Cloud Computing, Rennes, France

Enseignement

2020 **Sécurité Matérielle (3h30 CM, 3h30 TP)**, *Centrale Supélec, Rennes*.
Cours magistraux et travaux pratiques (5 étudiants, M2).

2020 **Sécurité (6h CM, 4h projet)**, *ENS Rennes*.
Cours magistraux et création de 6 projets par binômes (12 étudiants, L3).

2020 **Attaques par canaux auxiliaires (10h CM)**, *INSA Rennes*.
Cours magistraux (20 étudiants, M2).

2019 **Sécurité (6h CM, 2h projet)**, *ENS Rennes*.
Cours magistraux et création de 6 projets par binômes (12 étudiants, L3).

2019 **Attaques par canaux auxiliaires (10h CM + 6h TP)**, *INSA Rennes*.
Cours magistraux et travaux pratiques (10 étudiants, M2).

2018 **Attaques par canaux auxiliaires (10h CM + 6h TP)**, *INSA Rennes*.
Cours magistraux et travaux pratiques (10 étudiants, M2).

2017 **Projet veille technologique (eq. 19h TD)**, *Université de Rennes 1*.
Projet de veille technologique sur les canaux cachés utilisant la micro-architecture (4 étudiants, M2).

2016, 2017 **Embedded security (2 $\times$ 7.5h CM)**, *TU Graz, Autriche*.
Cours magistraux (en anglais). Participation à la création du cours, production et correction de l'examen final pour tous les étudiants (50 étudiants, master).

2014 **Programmation orientée objet en Java (14h TD + 14h TP)**, *INSA Rennes*.
Cours et travaux pratiques (groupe de 28 étudiants, L2). Correction hebdomadaire des travaux pratiques. Participation à la production et à la correction de l'examen final (110 étudiants).

2013 **Introduction à la programmation orientée objet en Java (14h TD + 13h TP)**, *INSA Rennes*.
Cours et travaux pratiques (groupe de 29 étudiants, L1). Correction hebdomadaire des travaux pratiques. Participation à la production et à la correction de l'examen final (280 étudiants).