Clémentine MAURICE

CNRS researcher in computer science

✉ *clementine.maurice@irisa.fr*
cmaurice.fr

Research Interests

My research interests span the areas of **micro-architectural side and covert channels**, which exploit timing differences introduced at the hardware level, as well as **software-based fault attacks**. My research aims at building more efficient and more robust countermeasures against these types of attacks. A first and necessary step is to find new attack vectors on modern commodity devices such as servers, laptops, desktops and mobile devices, as well as to minimize the requirements for attacks to fit more realistic scenarios (e.g., cross-CPU, without any shared memory, in virtualized environments). As these attacks exploit complex and undocumented processor components, my research also encompasses reverse-engineering hardware components.

Curriculum Vitae

since 2017 **CNRS researcher**, *EMSEC group, IRISA*, France.

2016–2017 **Postdoctoral researcher**, *Secure Systems group, IAIK, TU Graz*, Austria.

2012–2015 **PhD student**, *Technicolor and Eurecom*, Cesson-Sévigné and Sophia Antipolis, France.
PhD Thesis: Information leakage on shared hardware: Evolutions in recent hardware, and applications to virtualization.
- June 2015: Two-week visit at the Secure Systems group, TU Graz, Austria. Adaptation of Rowhammer, a DRAM-based fault attack, in JavaScript.

2007-2012 **Student**, *INSA*, Rennes, France.
Double degree: Diplôme d'Ingénieur (equivalent MSc in engineering), and Master of Science in Computer Science. *Major*: Information and computing infrastructure security.
- 2012: Research internship and master thesis (six months), Technicolor, Security & content protection lab, Cesson-Sévigné, France. Improvement of 802.11 fingerprinting methods.
- 2011: Research internship (two months), Inria, Texmex group, Rennes, France. Transcript-based topic segmentation.

2007 **Baccalauréat Scientifique, magna cum laude**, *Lycée Descartes*, Rennes.

Publications

Computer science is a conference-driven domain, with very selective conferences. Conferences being recognized by peers as being in the top tier in computer science security are ACM CCS, IEEE S&P, USENIX Security and NDSS. My scientific visibility is reflected by my h-index of 17 according to Google Scholar which records 2270 citations (as of September 2020). Acceptance rate is given when known.

Peer-reviewed international journal articles

[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.

Peer-reviewed international conference articles

[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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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. Acceptance rate: 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.

Peer-reviewed international workshop articles

[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)*. colocated with EuroS&P. June 2020.

Public outreach articles

[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).

Patents

[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

Steering committee member of conferences and workshops
- Workshop on Offensive Technologies (WOOT) since 2020

Chairing of conferences and workshops — Core ranking given when known (`http://portal.core.edu.au/conf-ranks`)
- USENIX Security Symposium 2021, rank A*, **artifact evaluation committee co-chair**
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2020, rank C, **PC chair**
- Workshop on Offensive Technologies (WOOT) 2019 (colocated with Usenix Security), **PC co-chair**
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2019, rank C, **PC co-chair**

Program committee member of international conferences — Core ranking given when known (`http://portal.core.edu.au/conf-ranks`)
- IEEE Symposium on Security and Privacy (**S&P**) 2021, rank A*
- USENIX Security Symposium (**USENIX Sec**) 2020, rank A*
- IEEE Symposium on Security and Privacy (**S&P**) 2020, rank A*
- Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA) 2018, rank C
- International Conference on Distributed Computing Systems (**ICDCS**) 2018, Security track, rank A
- World Wide Web Conference (**WWW**) 2018, Security and Privacy research track, rank A*
- Conference on Cryptographic Hardware and Embedded Systems (**CHES**) 2018, rank A
- Annual Computer Security Applications Conference (**ACSAC**) 2017, rank A
- International Symposium on Engineering Secure Software and Systems (ESSoS) 2017

Program committee member of international workshops and national conferences
- 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 (colocated with Usenix Security)
- Symposium sur la sécurité des technologies de l'information et des communications (SSTIC) 2018

Reviewer
- 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

External reviewer : 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

Community service
- Vice chair for the PhD thesis award of the French computer science society (SIF), 2019, 2020
- Jury member for the PhD thesis award of the French computer science society (SIF), 2018
- Hiring committee member for the Assistant Professor position at INSA de Toulouse, 2018

Event organization
- Organization of a summer school on the Security of Software / Hardware Interfaces, 2019, Rennes, France
- Publicity for the spring school on Security & Correctness in the IoT 2017, Graz, Austria
- On-site for COSADE 2016, Graz, Austria

PhD committees

- 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, December 2020
- Radhesh Konoth, "Vulnerable by Design: Mitigating Design Flaws in Hardware and Software", VU Amsterdam, Netherlands, December 2020
- Pepe Vila, "Learning Secrets and Models from Execution Time", IMDEA Software Institute, Spain, June 2020
- Antoine Vastel, "Tracking Versus Security: Investigating the Two Facets of Browser Fingerprinting", Université de Lille, France, October 2019
- Fabio Pagani, "Advances in memory forensics", EURECOM, France, September 2019

Student supervision

PhD students

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

Postdocs

- Sam Thomas, 2018-2019

Master students

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

Projects

2019–2023 **ANR JCJC** MIAOUS (PI)
2019–2023 ANR ARCHI-SEC (local PI)
2019–2023 ANR MobiS5 (member)
2018 PEPS JCJC INS2I installation grant
2018–2020 DGA grant

Awards

2018 **Young researcher award**: Prix Bretagne Jeune Chercheuse et Chercheur, high-tech category.
2015 DIMVA **Best paper** award for [18].

Presentations

I presented my work in **international research groups seminars** (e.g., Vienna, Bochum), in **summer schools** for young researchers, and to major **industry vendors** (Intel, Qualcomm). Moreover, I presented my work in **non-academic hacker conferences** (e.g., Chaos Communication Congress, BlackHat Europe, or Rencontres Mondiales du Logiciel Libre), which gather academic and industry researchers, as well as technology enthusiasts. The audience is therefore diverse and can be quite large (12 000 participants at the Chaos Communication Congress in Hamburg).
The complete list of my presentations is available on my web page: `https://cmaurice.fr`

2020 Masterclass at the International Cybersecurity Forum (FIC), Lille, France
2019 Invited presentation at the FICHSA conference, Tel Aviv, Israel
Invited lecture at the Ben-Gurion University of the Negev, Beer Sheva, Israel
Invited presentation at the Security day, INSA Toulouse, France
2018 Invited presentation at the 8th Inria/Technicolor Workshop On Systems (WOS8), Rennes, France
Invited presentation at Séminaire du DIT, ENS Rennes, France
Invited lecture (Skype) at the Indian Institute of Technology Kanpur, India
Invited presentation at Séminaire Sécurité du LORIA, Nancy, France
Invited lecture (lab) at the Cyber in Occitanie summer school, Montpellier, France
Invited presentation at Colloque Architecture, Toulouse, France
Invited presentation at Journées nationales pré-GDR Sécurité Informatique, Paris, France
2017 Presentation at RMLL 2017, Saint-Étienne, France
Invited presentation at SSTIC 2017, Rennes, France
Lecture at the spring school Security & Correctness in the IoT, Graz, Austria
Presentation at RuhrSec 2017, Bochum, Germany

Keynote at XDOM0 2017 (workshop colocated with EuroSys), Belgrade, Serbia
Invited presentations at Intel, Hillsboro, Oregon, USA
Invited presentation at Qualcomm, San Diego, California, USA

2016 Presentation at the Chaos Communication Congress (33C3), Hambourg, Germany
Invited presentation at SBA Research, Vienna, Austria
Invited lecture at the HackerPraktikum, Ruhr-University Bochum, Germany
Invited presentation at Ruhr-University Bochum, Germany
Presentation at BlackHat Europe 2016, London, UK
Invited lecture at the IPICS 2016 summer school in KU Leuven, Belgium

2015 Presentation at the Chaos Communication Congress (32C3), Hambourg, Germany
Invited presentation at the Secure Systems group seminar, TU Graz, Austria

2013 Presentation at the 3rd Workshop on Storage and Cloud Computing, Rennes, France

Teaching

winter 2020 **Hardware security**, *Centrale Supélec, Rennes*, Lecturer.
Lectures and labs for an elective master course (5 students).

winter 2020 **Security**, *ENS Rennes*, Lecturer.
Lectures and projects for an elective bachelor course (12 students).

winter 2020 **Side-channel attacks**, *INSA Rennes*, Lecturer.
Lectures and labs for an elective master course (20 students).

winter 2019 **Security**, *ENS Rennes*, Lecturer.
Lectures and projects for an elective bachelor course (12 students).

winter 2019 **Side-channel attacks**, *INSA Rennes*, Lecturer.
Lectures and labs for an elective master course (11 students).

winter 2018 **Side-channel attacks**, *INSA Rennes*, Lecturer.
Lectures and labs for an elective master course and labs (10 students).

winter 2017 **Technology watch project**, *Université de Rennes 1*.
Supervising a group of students for a project on microrachitectural covert channels (4 students).

spring 2016, spring 2017 **Embedded security**, *TU Graz, Austria*, Co-lecturer.
Lectures for an elective master course. Participating in the creation of the course, and production and grading of the final examination for all students (50 students).

spring 2014 **Object-oriented programming with Java**, *INSA Rennes*, Teaching assistant.
Lectures and labs for a group of 28 students. Weekly correction of labs for 7 teams. Participating in the production and grading of the final examination for all groups (110 students).

spring 2013 **Introduction to object-oriented programming with Java**, *INSA Rennes*, Teaching assistant.
Lectures and labs for a group of 29 students. Weekly correction of labs for 7 teams. Participating in the production and grading of the final examination for all groups (280 students).