32 Vassar St, Office 32-G890
Cambridge 02139, MA

JULES DREAN

drean.io

drean@mit.edu
Last Updated: February 2024

SUMMARY

I am a 6th year PhD student at MIT CSAIL and I build computers and systems that have interesting security properties. More precisely, my research intersects trusted hardware, applied cryptography and micro-architectural side channels.

EDUCATION

Boston, USA — **Massachusetts Institute of Technology - PhD Program** — **2020 - Present**
- PhD student in the Electrical Engineering and Computer Science Department.
- Co-advised by Professors Srini Devadas and Mengjia Yan from the Computer Science and Artificial Intelligence Lab.

Boston, USA — **Massachusetts Institute of Technology - Master of Science** — **2018 - 2020**
- Electrical Engineering and Computer Science Department. GPA : 5.00
- Co-advised by Professors Srini Devadas and Mengjia Yan from the Computer Science and Artificial Intelligence Lab.
- Master Thesis: "*CaSA: End-to-end Quantitative Security Analysis of Randomly Mapped Caches.*"

Paris, France — **Telecom Paris - Master Program** — **2016 - 19**
- Top French Engineering School in Electrical Engineering and Computer Science.
- Second year : Majors in Embedded Systems, Theoretical Computer-Science, Maths and Operational Research.
- GPA : 3.99/4.00

Paris, France — **Lycée Henri IV - Bachelor Level Program** — **2014 - 16**
- Classe Préparatoire, Major in Mathematics and Physics. Intensive program to entry French engineering schools.
- MPSI - MP* - admittance rate < 2%.

PUBLICATIONS

- Cook, J., **Drean, J.**, Behrens, J., & Yan, M. "*There's Always a Bigger Fish: A Clarifying Analysis of a Machine-Learning-Assisted Side-Channel Attack.*" In *2022 ACM/IEEE International Symposium on Computer Architecture* ***(ISCA 2022).*** **ACM/ IEEE - MICRO Top Picks 2023**
- Deutsch, P., Yuheng, Y., Bourgeat, T., **Drean, J.**, Emer, J., & Yan, M. "*DAGguise: Mitigating Memory Timing Side Channels.*" In *2022 ACM International Conference on Architectural Support for Programming Language and Operating Systems* ***(ASPLOS 2022).*** **ACM**
- Bourgeat, T.* , **Drean, J.***, Yang, Y., Tsai, L., Emer, J., & Yan, M. ***co-first authors** "*CaSA: End-to-end Quantitative Security Analysis of Randomly Mapped Caches.*" In *2020 53rd Annual IEEE/ACM International Symposium on Microarchitecture* ***(MICRO 2020).*** **IEEE. - Finalist for the Intel Hardware Security Award 2021**
- Lebedev, I., Hogan, K., **Drean, J.**, ... & Devadas, S. "*Sanctorum: A lightweight security monitor for secure enclaves.*" In *2019 Design, Automation & Test in Europe Conference & Exhibition* ***(DATE 2019).*** **IEEE**
- Neuman, S. M., Koolen, T., **Drean, J.**, Miller, J. E., & Devadas, S. "*Benchmarking and workload analysis of robot dynamics algorithms.*" In *2019 IEEE/RSJ International Conference on Intelligent Robots and Systems* ***(IROS 2019).*** **IEEE**

WORK AND RESEARCH EXPERIENCE

Boston, USA — **Massachusetts Institute of Technology** — **September 2018 - Present**
- Research Interest : Computer Security, Hardware Security, Applied Cryptography, and Secure Processors.
- Currently working on hardware/software platform to accelerate cryptographic protocols, while providing integrity.
- Past projects: Citadel - Enclave platform for the RISC-V architecture. CaSA - Developed model to simulate randomly mapped cache behavior during timing side-channel attack. Bigger Fish - micro-architectural side channel analysis.

Seattle, USA — **Microsoft Research** — **May - August 2023**
- Research Intern - Cloud and Infrastructure Security Group - Advised by Marcus Peinado and Sangho Lee
- Worked on securing cloud computing using novel Smart NICs technologies.

Boston, USA — **Nvidia** — **May - August 2022**
- Research Scientist Intern - NVResearch Architecture group - Worked under the supervision of Aamer Jaleel.
- Worked on new hybrid schemes to accelerate multi-party computation using confidential computing.

Boston, USA — **Gradient Tech** — **May - September 2019**
- System Engineer Intern
- Worked on Trusted Execution Environment and Secure Boot on ARM architecture.

Paris, France — **Telecom Paris** — **September - July 2018**
- Master Research Project with Prof. Laurent Sauvage
- Development of a simulation tool for laser probing technique and fault injection and side-channel analysis.

Boston, USA **Cadence Design System** **July - September 2017**

- Software Engineer Intern.
- Design and implementation of a Physics based engine to solve multiple optimization problems in EDA.
- Reached and improved performance of existing designs. A team was selected to further develop the project.

TEACHING

Universidad Anáhuac Querétaro **Introduction to Computer Security** **January 2024**

- Created and taught a hacking workshop to four different student groups over the course of 3 weeks. The students learned fundamentals in mathematics, computer science, electronic and security to prepare them for a final challenge where they had to extract a long password from an Arduino using a timing side channel attack.

MIT **6.S060: Foundations of Computer Security** **Fall 2021**

- Helped create the class. Designed and implemented every labs and part of the course material with Derek Leung, including a protocol verification tool to auto-grade the labs. Gave weekly recitations and held office hours. Taught by Srini Devadas, Yael Kalai, Nickolai Zeldovich and Henry Corrigan-Gibbs.

AWARDS AND PRIZES

- **2023** MIT Graduate Student Change-Maker Award.
- **2020 - 2022** Google Fellowship Program in Trustworthy Computing.
- **2016** 3rd price of the Sopra Steria - Institut de France Foundation Price. Development of a device to monitor elders' health. A first step to make home hospitalization more accessible.
- **2014** French National Baccalauréat with distinction. - Special mention from the Jury. Average : 19.5/20.
- **2010** Award winner of Life & Science Junior - « Innovez » competition. Guitar amplifier emulator on a mobile phone. Youngest winner of the year and prize of a thousands euros for further research.

LEADERSHIP AND MENTORING

Mentor and Supervisor **MIT Math & CS PRIMES Program** **Spring 2021 - Present**

Graduate students mentor high school students to do research in CS over several years. Over the last year, I've worked with Rachel and taught her basic computer architecture, cryptography, complexity theory and the required mathematical foundations. We then started working on trusted hardware and virtual assets. We've developed a prototype and are now close to submit our work to a conference.

Mentor and Supervisor **MIT UROP Program** **Fall 2020 - Present**

Top undergrad students engage in grad-level research projects. I am helping Jack and Miguel to develop various new attacks on operating systems and have already got one paper accepted.

Board Member and Social Chair **MIT-EECS THRIVE** **Fall 2020 - Present**

An association of students from the EECS department that advocate for Diversity, Equity, Inclusion and Mental Health. We've developed several initiatives and collaborations with internal and external actors.

Mentor **MIT-EECS GAAP Program** **2020 - Present**

Graduate students help students from all over the world and from underrepresented backgrounds to apply for graduate school in the US. I've been mentoring three students over the past two years.

CODING EXPERIENCE

- Bare metal programming - Low-level System Programming - Competitive Programming - Hardware Programming.
- Proficient in C, C++, Assembly Code (RISCV, ARM, X86), Java, Python, Blue Spec, Verilog, System C.

OTHER SKILLS AND INTERESTS

- **Sports and Occupations:**
  Former ballet dancer at the National Conservatory of Brittany.
  Currently swimming, running and learning Muay Thai and Brazilian Jui-Juitsu.
  I also enjoy practicing photography, cooking and studying Queer, Gender and Women studies at MIT.
- **Languages :**
  French: Native | English: Bilingual | Spanish: Advanced.