DANIEL
DE ALMEIDA BRAGA

EDUCATION & EXPERIENCES

Research Engineer (Capsule team) *Since 05/2024*
INRIA, Rennes, France

Postdoc/Visiting Researcher *10/2022-09/2023*
IRISA, Rennes, France
Visting Daniel Gruss (TU Graz, Austria), Clémentine Maurice (Lille University, France) and Sébastien Bardin (CEA Saclay, France). Still employe in Rennes.
Artifact reviewer for USENIX Security 2023

PhD Student in Computer Science *10/2019-09/2022*
IRISA, Rennes, France
"Cryptography in the Wild: The Security of Cryptographic Implementations"
Jury: S. Bardin, K. Paterson, Y. Yarom (reviewers), S. Blazy, S. Duquesne, C. Maurice (examinors), PA. Fouque and M. Sabt (Advisors)

Security Analyst *09/2018-09/2019*
Amossys, Rennes, France
Evaluation of cryptography-related softwares for certification

Master Of Cryptography with honors *2016-2018*
University of Rennes

Bachelor of Mathematics with honors *2013-2016*
University of Angers

Baccaleuréat S with highest honors *2010-2013*
Lycée d'Estournelles de Constant, La Flèche, France

AWARDS

2023 Best thesis award Fondation Rennes 1
2022 Google PhD Fellowship
2021 ProtonMail Security Contributor
2020 2nd place at CSAW Applied Research Europe

INVITATIONS & TALKS

2023
- EuroS&P, Deflt, Netherland
- Service: Usenix Artifact reviewer

2021
- IRMAR seminar, Rennes, France
- CEA seminar, Saclay, France
- CCS, Online
- Workshop Attack on Crypto (WAC), Online
- EDUC seminar, Online
- Quarklab seminar, Rennes, France
- REDOCS: Privacy in IoT (hackathon)

2020
- CSAW Applied Research, Online
- ACSAC, Online
- TCHES, Online
- GlobalPlatform Committe, Online

ABOUT ME

My research focuses on vulnerabilities in cryptographic implementations, related to the core protocol or its implementation (side channel). I also studied side-channel mitigation tools deployment (human factor-centered study), and formally verified implementations.

SKILLS

- Side channel attacks
- Microarchitecture (CPU, GPU)
- Software analysis (fuzzing, constant time verification, ...)
- OS internals (mostly Linux)
- Reverse Engineering basics
- Programming (C, Python, Bash)
- Teaching & mentoring
- Seminar organization
- Technical communication

CONTACT

ddealmei.0@gmail.com
ddealmei.github.io

PUBLICATIONS

"These results must be false": A usability evaluation of constant-time analysis tools — *Rank A**

Marcel Fourné, Daniel De Almeida Braga, Jan Jancar, Mohamed Sabt, Peter Schwabe, Gilles Barthe, Pierre-Alain Fouque and Yasemin Acar
USENIX Security 2024

Generic and Automated Drive-by GPU Cache Attacks from the Browser — *Rank A*

Lukas Giner, Roland Czerny, Christoph Gruber, Rausher Fabian, Andreas Kogler Daniel De Almeida Braga, Daniel Gruss

ACM AsiaCCS 2024 - **Best paper award**

From Dragondoom to Dragonstar: Side-channel Attacks and Formally Verified Implementation of WPA3 Dragonfly Handshake — *Rank A*

Daniel De Almeida Braga, Natalia Kulatova, Mohamed Sabt, Pierre-Alain Fouque and Karthikeyan Bhargavan
IEEE EuroS&P 2023

"They're not that hard to mitigate": What Cryptographic Library Developers Think About Timing Attacks — *Rank A**

Jan Jancar, Marcel Fourné, Daniel De Almeida Braga, Mohamed Sabt, Peter Schwabe, Gilles Barthe, Pierre-Alain Fouque and Yasemin Acar
IEEE S&P 2022

PARASITE: PAssword Recovery Attack against Srp Implementations in ThE wild — *Rank A**

Daniel De Almeida Braga, Pierre-Alain Fouque and Mohamed Sabt
CCS 2021

Dragonblood is Still Leaking: Practical Cache-based Side-Channel in the Wild — *Rank A*

Daniel De Almeida Braga, Pierre-Alain Fouque and Mohamed Sabt
ACSAC 2020

The Long and Winding Path to Secure Implementation of GlobalPlatform SCP10 — *Rank A*

Daniel De Almeida Braga, Pierre-Alain Fouque and Mohamed Sabt
TCHES 2020