



INTRODUCTION TO CACHE SIDE-CHANNEL ATTACKS

le 9 octobre 2018 16h00 - 18h00

ENS Rennes, Salle du conseil
[Plan d'accès](#)

Intervention de **Clémentine Maurice**, CR CNRS, équipe **Emsec** (IRISA, Rennes), dans le cadre des séminaires du département Informatique et télécommunications.



Hardware is often considered as an abstract layer that behaves correctly, just executing instructions and outputting a result. However, the internal state of the hardware leaks information about the programs that are executing, paving the way for covert channels or side-channel attacks. Secret information includes cryptographic secrets, as well as less obviously sensitive data, such as memory addresses that can be used by attackers to bypass vulnerability mitigations put in place to defend against other types of vulnerability (e.g. KASLR).

In this presentation, I will give an introduction to cache side-channel attacks. I will start by presenting the building blocks of these attacks, explaining the different challenges one has to overcome in order to perform them on modern hardware. As these attacks require a very good understanding of the underlying (and often undocumented) hardware components, I will explain how we reverse-engineered some parts of the CPU cache. I will then show some practical applications, and will conclude by presenting countermeasures as well as open challenges in this field.

THÉMATIQUE(S)

Formation, Recherche - Valorisation

CONTACT

[Luc Bougé](#)

À LIRE AUSSI



Séminaire de Claire Vernade



Séminaire de Sam Thomas



Séminaire de Emmanuelle Anceaume

CONTACT

ARCHIVES

[Séminaires 2018-2019](#)
[Séminaires 2017-2018](#)
[Séminaires 2016-2017](#)
[Séminaires 2015-2016](#)
[Séminaires 2014-2015](#)
[Séminaires 2013-2014](#)
[Séminaires 2012-2013](#)
[Séminaires 2011-2012](#)
[Séminaires 2010-2011](#)
[Séminaires 2009-2010](#)
[Séminaires 2008-2009](#)
[Séminaires 2007-2008](#)
[Séminaires 2006-2007](#)
[Séminaires 2005-2006](#)
[Séminaires 2004-2005](#)
[Séminaires 2003-2004](#)
[Séminaires 2002-2003](#)