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 outputing 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

Open Science needs a Universal Software Archive: Enter Software Heritage

Apprentissage automatique et respect de la vie privée

Function approximation problems in signal processing and deep learning

DOCUMENTATION

Vous souhaitez recevoir plus d'information sur l'ENS Rennes, vous pouvez pour cela remplir le formulaire de demande de documentation.