UNIVERSIDAD COMPLUTENSE MADRID

Facultad de Informática

ANUNCIO DE CONFERENCIA

POSGRADO

Hardware/software security contracts: Principled foundations for building secure microarchitectures

Marco Guarnieri
IMDEA Software

Facultad de Informática
on-line https://meet.google.com/bcr-pssw-xdb
jueves 9 de diciembre de 2021 - 17:00

Resumen:

Microarchitectural attacks, such as Spectre and Meltdown, are a class of security threats that affect almost all modern processors. These attacks exploit the side-effects resulting from processor optimizations to leak sensitive information and compromise a system's security. Over the years, a large number of hardware and software mechanisms for preventing microarchitectural leaks have been proposed. Intuitively, more defensive mechanisms are less efficient, while more permissive mechanisms may offer more performance but require more defensive programming. Unfortunately, there are no hardware-software contracts that would turn this intuition into a basis for principled co-design. In this talk, we present a framework for specifying hardware/software security contracts, an abstraction that captures a processor's security guarantees in a simple, mechanism-independent manner by specifying which program executions a microarchitectural attacker can distinguish.

Sobre Marco Guarnieri:

Marco Guarnieri is an Assistant Research Professor at IMDEA Software Institute (Spain). He holds a PhD in Computer Science from ETH Zurich (Switzerland). His research focuses on the design, analysis, and implementation of practical systems for securely storing and processing sensitive data. He applies his research to the analysis of micro-architectural side-channel attacks (and countermeasures) and to database security.