I SEMINARI DEL DII

CYBER master SECURITY

Speculative Execution Vulnerabilities:
Caratteristiche Tecniche, Impatto e Contromisure

Dario Faggioli - SUSE Software Solutions Italy

VENERDÌ 23 LUGLIO
H 10:00
QR code per accesso

Abstract

Sono state rese note al mondo nell'ormai lontano 2018, ma di vulnerabilità legate alla esecuzione speculativa si parla ancora oggi. Infatti, l'idea che sia possibile accedere a dati riservati sfruttando non un bug nel software ma alcune caratteristiche intrinseche di come le CPU moderne provano a garantirci prestazioni elevate, ha rappresentato un vero e proprio cambio di paradigma. Non stupisce quindi il fatto che, dopo Meltdown e Spectre, ne sono state e continuano e venirne scoperte di nuove - alcune anche più gravi delle due originali, come ad esempio L1TF ed MDS. Questo seminario si propone di offrire una panoramica su questo tipo di vulnerabilità: cosa le rende possibili, quali meccanismi di protezione permettono di scavalcare e qual è il loro impatto (sia su sistemi fisici sia nell'ambito di tecnologie quali virtualizzazione e container) nonché quali sono le contromisure che sono state e stanno tuttora venendo adottate.

Bio

Dario Faggioli ha conseguito la Laurea Magistrale in Ingegneria Informatica, nel 2007, ed "Diploma di Perfezionamento" in "Innovative Technologies of ICT and Robotics", nel 2012. Dal 2011 si occupa di virtualizzazione e dal 2018 lavora presso SUSE. Partecipa allo sviluppo del kernel Linux (è co-autore dello scheduler real-time noto come SCHED_DEADLINE), degli hypervisor Xen e KVM, e anche di QEMU, libvirt ed altri progetti. Partecipa, spesso con presentazioni, alle principali conferenze ed eventi del mondo Open Source quali Open Source Summit, KVM Forum, Xen Summit o Linux Plumbers.

Il link per partecipare è il seguente: https://tinyurl.com/2jbpekdd

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

In collaborazione con

IIT Istituto di Informatica e Telematica

UNIVERSITÀ DI PISA