I SEMINARI DEL DII

CYBER master SECURITY

Confidential Computing. Perché fidarsi è bene... Ma criptare la memoria delle macchine virtuali è meglio

Dario Faggioli - SUSE Software Solutions Italy

VENERDÌ 14 OTTOBRE
H 10:00
QR code per accesso

Abstract

L'utilizzo di macchine virtuali (VM) è spesso dettato da ed associato alle garanzie di maggior sicurezza che offre tra esse ed il sistema host, che i sistemi di virtualizzazione definiscono ed implementano; fino ad oggi, tuttavia, non era possibile fornire altrettante elevate garanzie di riservatezza dei dati gestiti all'interno delle VM. Infatti era impossibile, fino ad oggi, rendere sicuri i dati nel momento in cui vengono caricati in memoria e/o nei registri del processore durante l'esecuzione della macchina virtuale. L'insieme di tecnologie che permettono di raggiungere anche quest'ultimo livello di protezione, vanno sotto il nome di Confidential Computing: è grazie ad esse che è possibile garantire a tutto tondo la riservatezza dei dati che le VM manipolano, anche nei confronti di chi gestisce il server di virtualizzazione (e/o il servizio di Cloud Computing) e ne controlla quindi l'hypervisor. Questo seminario si propone di fornire le informazioni necessarie per comprendere i concetti alla base del Confidential Computing, oltre che alcune nozioni tecniche sulle tecnologie che lo rendono possibile. Verranno mostrati, inoltre, alcuni semplici esempi pratici della sua efficacia e illustrate alcune indicazioni su come renderlo operativo su sistemi di virtualizzazione basati sull'hypervisor KVM.

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/2a9w8k48

DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE

In collaborazione con

Istituto di Informatica e Telematica

UNIVERSITÀ DI PISA