CBG | Cyber@ Ben-Gurion University of the Negev | המרכז לחקר הגנת הסייבר באוניברסיטת בן-גוריון בנגב

Cyber Security Seminar

Cyber@ Ben-Gurion is located at the Advanced Technologies Park, next to Telekom Innovation Laboratories, where it is nurtured in the hothouse of innovation that exists there. In the activities center, our leading researchers will deliver seminars that deal with Cyber Security subjects. The seminars will take place every two/three weeks.

You are invited to attend our seminar-

The talk will take place on Wednesday, 15.11.17 at 13:00 in building 37,

2nd floor, 202 Auditorium , Ben-Gurion University of the Negev.

The seminar will be managed by: **Dr. Gabriel Scalosub**

Who will give an in-depth review on the subject

Towards Hardening Virtualization Against Cache Side-Channel Attacks

Abstract:

The ubiquitiousness of virualized environments, and specifically the increasing usage of cloud-based services, poses various security threats to both infrastructure providers, as well as customers. The agility and economic benefits of an IaaS allowing the setting up of services on the fly, come with various risks, including such based on trust, privacy issues, and the threat of information leakage. One of these potential hazards is the existence of side-channels that emerge in the system, due to, e.g., ill-defined procedures, un-patched SW modules, or the mere usage of shared resources by the different customers/applications. One such predominant example is cache side-channels, which arise from the fact that multiple tenants co-located on a single physical host inherently make use of a shared last-level cache. Attacks based on such side channels have been shown to allow a malicious co-located VM to acquire private information associated with a different VM operating on the same physical host. We present a full-fledged implementation of such an attack, and highlight some of its inherent properties. Based on these properties, we design mechanisms that are targeted at thwarting such attacks. These mechanisms are expected to operate as a service on the hypervisor level, and require no code change by an application running in a VM, nor any specialized hardware modules. We discuss their design, and present some preliminary results as to their operation.

Fax. 08-6428016 .פקס | Tel. 08-6428005 .טל

Israel ישראל | Beer-Sheva 8470912 באר-שבע

אוניברסיטת בן-גוריון בנגב בחירה מצוינ