Cryptographic Engineering Research Group Presents

ECE DEPARTMENTAL SEMINAR

Exploiting Cache-based Side Channels in Public Clouds

Tuesday, August 11th, 2015
3:00 pm — 4:00 pm
Engineering Building, Room 3507

Speaker: Thomas Eisenbarth
Assistant Professor,
Worcester Polytechnic Institute, Worcester, MA

Abstract:

Cloud computing services are more popular than ever with their ease of access, low cost and real-time scalability. Security of the cloud computing infrastructure relies on logical isolation between virtual machines through sandboxing. However, isolation is not perfect, and side channels caused by the CPU's microarchitecture can result in information leakage across virtual machines. For instance, cache attacks that exploit access time variations when retrieving data from the cache or the memory are a powerful tool to extract information from a co-located virtual machine. In this talk, we present several methods of how to exploit cache-based side channels across VM boundaries. It will be shown how the Flush+Reload and Prime and Probe attack techniques can be applied to extract sensitive information from a co-located VM across cores, including information about used cryptographic libraries, but also more fine-grain information such as AES keys. Potential mitigation techniques to prevent these kind of attacks are also discussed. This talk is based on joint work with Gorka Irazoqui, Mehmet Sinn Inci, Berk Gulmezoglu and Berk Sunar.

Biography:

Thomas Eisenbarth is assistant professor at the Department of Electrical & Computer Engineering at WPI. His research interests include embedded systems security, efficient and secure implementation of cryptographic algorithms, physical attacks and countermeasures. Before joining WPI he spent two years at the Center for Cryptology and Information Security (CCIS) at Florida Atlantic University. He received his Ph.D. in Electrical and Computer Engineering from Ruhr University Bochum, Germany where he worked as a member of the Horst Goertz Institute for IT Security.