Title: Cache attacks against the Android TrustZone

Speaker: Avishai Wool

Abstract: The ARM TrustZone is a security extension helping to move the ``root of trust" further away from the attacker, which is used in recent Samsung flagship smartphones. These devices use the TrustZone to create a Trusted Execution Environment (TEE) called a Secure World, which runs secure processes called trustlets. The Samsung TEE includes cryptographic key storage and functions inside the Keymaster trustlet.

We start by providing a critical review of Samsung's proprietary TrustZone architecture. We describe the major components and their interconnections, focusing on their security aspects. During this review we identified some design weaknesses, including one actual vulnerability. Next, we identify that the ARM32 assembly-language AES implementation used by the Keymaster trustlet is vulnerable to cache side-channel attacks. We successfully demonstrate cache attacks on a real device, against AES-256, on the Keymaster implementation, and present a technique for mounting side-channel attacks against AES-256 in GCM mode. Finally, we make significant progress towards realistic cache attacks on the AES implementation within the Secure World.

The talk will be based our recent papers SAC'18 and ESORICS'18 papers.

Joint work with Ben Lapid.

Bio: Prof. Avishai Wool is a professor in the School of Electrical Engineering at Tel Aviv University. He is also deputy-director of the Interdisciplinary Cyber Research Center at TAU. He received a B.Sc. in Mathematics and Computer Science with honors from Tel Aviv University (1989). He has a M.Sc. (1992) and a Ph.D. (1997), both in Computer Science from the Weizmann Institute of Science. His research interests include computer, network, and wireless security, SCADA systems, smart-card and RFID systems, sidechannel cryptanalysis, and firewall technology. Prior to joining Tel Aviv University, Prof. Wool spent four years as a Member of Technical Staff at Bell Laboratories, Murray Hill, NJ, USA. In 2000 he co-founded Lumeta Corp. In 2003 he co-founded AlgoSec Systems, a network security company, for which he continues to serve as Chief Technical Officer. He has published more than 110 research papers and holds 15 US Patents. He advised 3 Ph.D. and 35 M.Sc. students, and has served on the program committee of the leading IEEE and ACM conferences on computer and network security.