Title: What if your phone's battery could talk? Inference attacks using malicious battery

Speaker: Mark Silberstein

Abstract: Mobile devices are equipped with increasingly smart batteries designed to provide responsiveness and extended lifetime. However, such smart batteries may present a threat to users' privacy. We demonstrate that the phone's power trace sampled from the battery at 1KHz holds enough information to recover a variety of sensitive information. We show techniques to infer typed characters to reduce the password search space; to accurately recover browsing history in an open-world setup; to reliably detect incoming calls and the photo shots including their lighting conditions. Combined with a novel exfiltration covert channel that allows communication from the battery directly to a remote server without installing software on the phone, these attacks turn the malicious battery into a stealthy surveillance device. We deconstruct the attack by analyzing its robustness to sampling rate and execution conditions, and identify the sources of the information leakage to find the best way to defend against the attacks. We discover that an attacker can distinguish the browsed website by observing the GPU or DRAM power traces alone. However, the CPU and other power-hungry peripherals such as a touch screen are often the primary sources of fine-grain information leakage. We highlight the challenge to defend against the attacks by designing and evaluating several possible mitigation mechanisms. In summary, our work shows the feasibility of the malicious battery and motivates further research into system and application-level defenses to fully mitigate this emerging threat.

Based on the joint work with Pavel Lifshits and Mohit Tiwari presented at the Symposium on Privacy Enhancement Technologies (2018)

Bio: Mark Silberstein is an Assistant Professor in the department of Electrical Engineering at the Technion – Israel Institute of Technology. Mark's research is on Operating Systems for Heterogeneous Computer Systems with compute and I/O accelerators and near-data processing systems, as well as hardware side channels attacks and defenses. He's got his PhD in Computer Science at the Technion in 2011, and then rejoined the Technion EE department in 2013 as a faculty, where he is heading the Accelerated Computer Systems Lab.