Computing on Leaky and Faulty Platforms

Eran Tromer

School of Computer Science

Tel Aviv University

Tel Aviv 69978, Israel

Abstract:

Software, even impeccably programmed, depends on the underlying computer platform for its integrity and confidentiality. Corrupted platforms, or one that leak information, will violate expectations and may compromise security. This talk will survey two of our projects, studying different factets of this problem.

First, we will discuss the vulnerability of full-fledged PC computers to physical side-channel attacks. We observe that RSA secret keys can be extracted from PCs by a variety of unexpected physical channels, including acoustic eavesdropping using microphones, measurement of cable shield potential from afar, and even mere hand touch by a (suitably equipped) human attacker.

Turning to integrity, a promising approach to ensuring the integrity of computation (even when conducted on malicious platforms) is cryptographic proofs: SNARKs and Proof-Carrying Data. We will discuss feasibility, implementations, and initial applications to improving privacy in Bitcoin.