2018 Research Interest/Project Ideas

Byoungyoung Lee (byoungyoung@purdue.edu)

https://lifeasageek.github.io/

==========

Oblivex: ORAM based execution framework for Intel SGX

Recent reports have demonstrated that Intel SGX remains vulnerable to a number of memory-based side-channels including page table, cache and branch prediction attacks. In order to provide strong security guarantees, we propose Oblivex, an oblivious program execution framework, preventing general memory-based side-channel attacks. The key idea is to leverage ORAM-based operations to perform secure code execution and data access. Oblivex enforces compiler instrumentation to transform regular program layout into ORAM-compatible memory layout. Oblivex provisions its ORAM controller to perform data oblivious accesses in order to protect itself from the side-channel attacks.