Deniz Aytemiz

Paper Summaries

1. EnclaveDB: A Secure Database using SGX

Cloud environments get more pervasive as they are used as 3rd party computing services within many technologies. They are also the target of attackers who can exploit its database or operating system. One countermeasure for this is to use trusted execution environments or enclaves. Enclaves provide a secure environment where even the operating system cannot control or manage the code in the enclave, hence it is difficult to attack by malicious hosts. In this paper an architecture called EnclaveDB is proposed which leverages TEE (Trusted Execution Environment) by placing sensitive data to enclaves. It is a database that ensures confidentiality,integrity and freshness. It supports multiple party mode where multiple users are distrusted and hosts sensitive data and execute queries in the shared database. The experiments showed that with respect to a standard database EnclaveDB has significantly less overhead with up to 40% TPC-C.

2. Fidelius: Protecting User Secrets from Compromised Browsers

Many users enter important confidential information to their browsers such as credit card numbers, password etc. Browsers can set various opportunities for malicious parties to access these confidential information. In this paper a countermeasure called Fidelius, leveraging Trusted Execution Environment (TEE) technology as the underlying architecture. So even if the browser or operating system is under control by an attacker, enclaves in TEEs are safe from reach. Fidelius has three main components which are a trusted path to I/O from hardware enclaves, functionality running in the enclave and browser components that can interact with the enclave. The experiments show that the architecture has acceptable overhead and is able to successfully protect inputs (javascript execution, input from local storage, network connections) from fully compromised browsers.