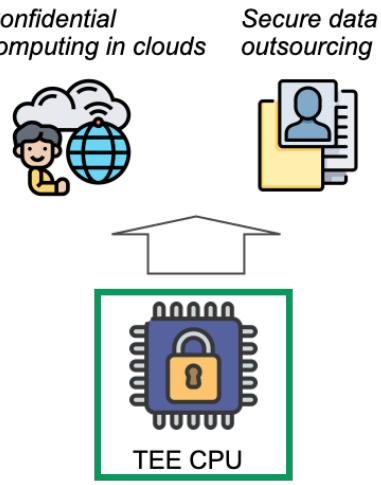
SaTC: CORE: Small: External Obliviousness in Trusted Execution Environments

Syracuse University

Challenge:

- How to support big-data computation with limited enclave memory while ensuring side-channel security.
- How to efficiently harden TEE/enclaves against memory-access pattern attacks

Side-channel secure TEE enables rest-assured confidential computing in the public clouds.

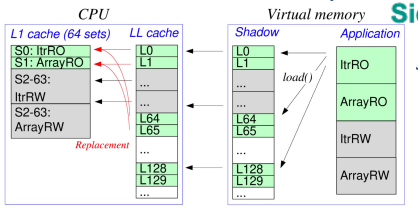


Scientific Impact:

- Efficient protection against memory-access pattern side-channels on SGX
- Systems support for oblivious data analytics
  - Aggregation, sorting and selection queries.

Solution:

- Dynamic program partitioning/execution framework in TSX/SGX
- Support various external oblivious algorithms
- Modeling cache and predict next $ miss



Broader Impact and Broader Participation:

- Cloud security industry; enabling confidential computing on third-party hosts
- Developed SGX/TEE labs and use them in courses
  - Receive Intel gift to further lab development
- Plan to release the tools in open-source repository

Project info (1922507, Syracuse University, contacts: ytang100@syr.edu)