CRII: SaTC: Rethinking Side Channel Security on Untrusted Operating Systems

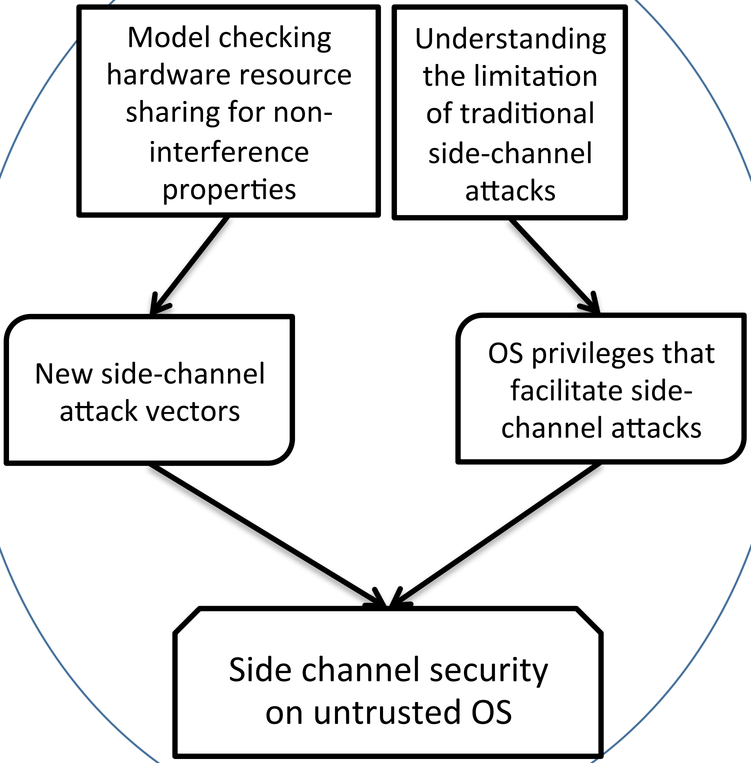
The Ohio State University

Challenge:

- Intel Software Guard eXtension (SGX) promises the confidentiality of software programs shielded in enclaves even when the operating system is untrusted
- Unfortunately, no systematic study of side-channel threats against the shielded execution on untrusted operating systems

Solution:

- Model checking to identify new side-channel attack vectors
- Systematically investigating OS privileges that facilitate side-channel attacks
- *Key innovation: Model checking techniques applied to automated detection of new side-channel attack vectors under the new threat model*



Model checking hardware resource sharing for non-interference properties
Understanding the limitation of traditional side-channel attacks
New side-channel attack vectors
OS privileges that facilitate side-channel attacks
Side channel security on untrusted OS

Scientific Impact:

- Advancing the state-of-the-art of side channel studies by exploiting model-checking techniques to automatically identify information leakage through shared hardware resources
- Systematic understanding of side-channel security against shielded execution on untrusted operating systems

Broader Impact:

- Knowledge of side-channel threats will be disseminated to industry vendors, including both SGX hardware manufacturers and software developers
- Introduction of side channel security into undergraduate security courses
- Involvement of underrepresented minority students in security research

Award # 1566444

The Ohio State University

Contact: Prof. Yinqian Zhang

(yinqian@cse.ohio-state.edu)