TWC:Small: Self-service Cloud Computing

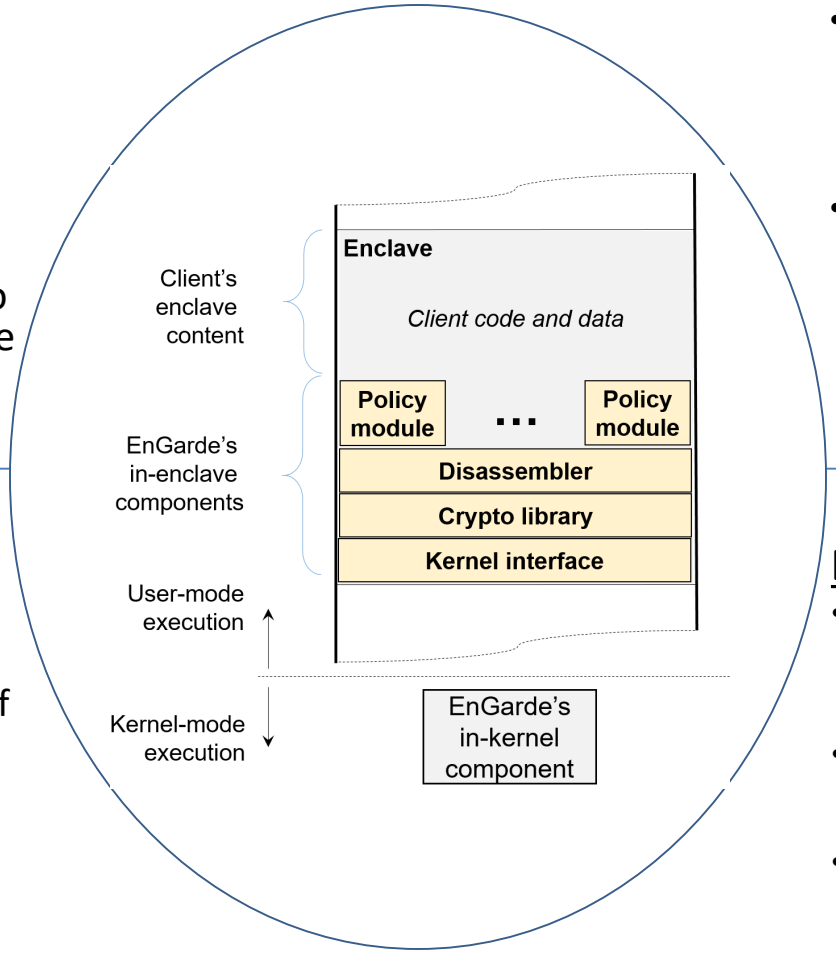
PI: Vinod Ganapathy, Rutgers University

Challenge:

- On public cloud platforms, client data exposed to untrusted cloud admins.
- Intel SGX addresses concerns, but cloud provider loses ability to monitor client's enclave code/data to check for regulatory compliance.

Solution:

- Developed a new *mutually-trusted abstraction* to ensure regulatory compliance of client code.
- Built ***EnGarde*** to implement and evaluate mutual trust atop OpenSGX.



Scientific Impact:

- Mutual trust allows cloud provider to examine client's code and data without compromising client's privacy.
- Ensures that client cannot violate regulatory compliance, thereby allowing cloud provider to exert some control over client enclaves.

Broader Impact:

- Intel SGX promises to dramatically improve client security and privacy on cloud platforms.
- But it flips the threat model and puts the cloud provider at a disadvantage.
- Mutual trust/EnGarde allows cloud provider to enforce regulatory compliance without compromising privacy of client code & data.

NSF-1420815, "TWC:Small:Self-service Cloud Computing,", PI: Vinod Ganapathy, Rutgers University, vinodg@cs.rutgers.edu