HARVARD
John A. Paulson School of Engineering and Applied Sciences

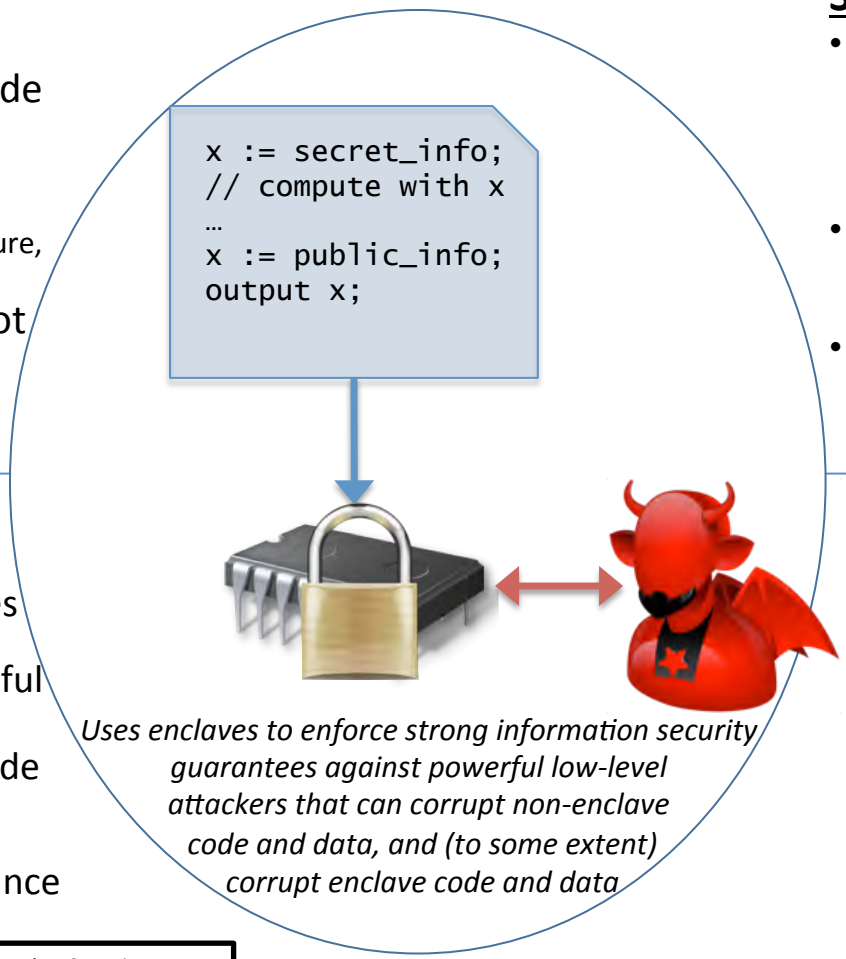
Automatic Enforcement of Expressive Security Policies using Enclaves

Challenge:

- Language-based techniques can provide strong information security guarantees
  - Noninterference, declassification, erasure, …
- But guarantees do not hold for powerful low-level attackers

Solution:

- Use hardware enclaves (e.g., Intel SGX) to protect against powerful low-level attackers
- Automatically infer code and data to place in enclaves to achieve security and performance



Uses enclaves to enforce strong information security guarantees against powerful low-level attackers that can corrupt non-enclave code and data, and (to some extent) corrupt enclave code and data

Scientific Impact:

- Extends application-specific information security guarantees to more powerful threat models
- Uses low-level hardware protection to enforce high-level security goals
- Automated inference facilitates use of enclaves

Broader Impact:

- Makes code and data more secure, against powerful attackers
- Increases usefulness of emerging hardware protection mechanisms
- Appeared at OOPSLA 2016

CAREER: Practical, Expressive, Language-based Information Security
Award number 1054172
PI: Stephen Chong, Harvard University
chong@seas.harvard.edu