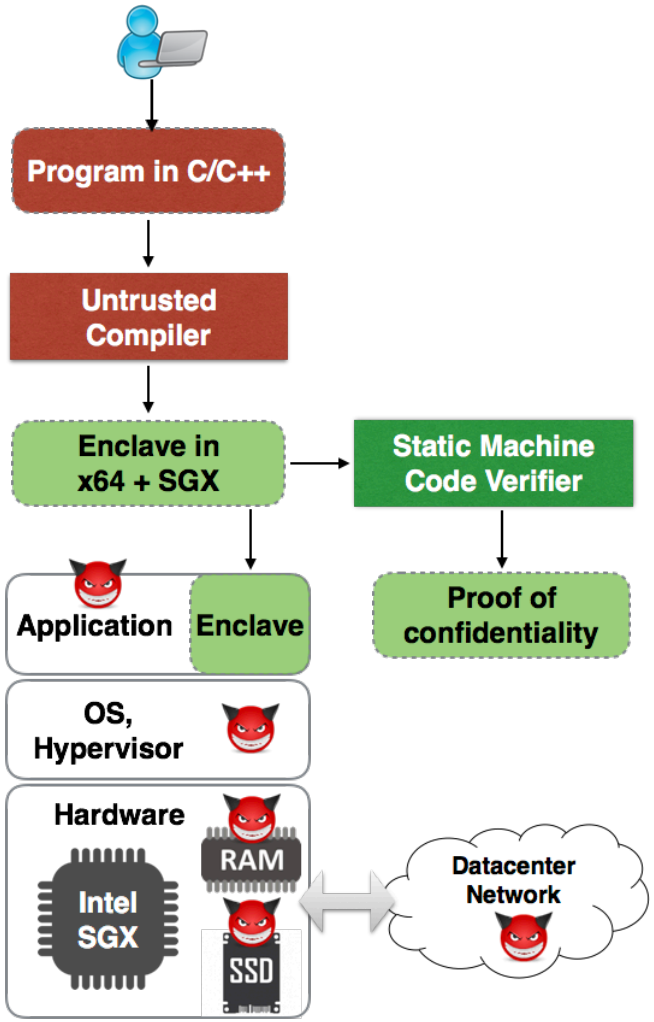
STARSS: Small: Collaborative: Specification and Verification for Secure Hardware

Challenge:

- Processors and SoCs increasingly built from untrusted components
- Systems software can be compromised → growing need for trusted hardware platforms

Solution:

- Security-aware hardware/ software verification
- Analysis and inference of specifications of hardware components and software-hardware interfaces
- Key innovation this year: Techniques for verifying software running on trusted hardware (e.g. Intel SGX)



STARSS Awards 1528108, 1525527
S. A. Seshia (UC Berkeley), R. E. Bryant (CMU).

Scientific Impact:

- Developing a foundation for formal and semi-formal specification and verification of secure hardware and software-hardware platforms
- Developing theories, threat models, tools, and benchmarks for security-aware hardware design

Broader Impact:

- Significantly improve security and privacy guarantees by enhancing trust in platforms
- Develop modules to teach students to design systems with formal security mindset