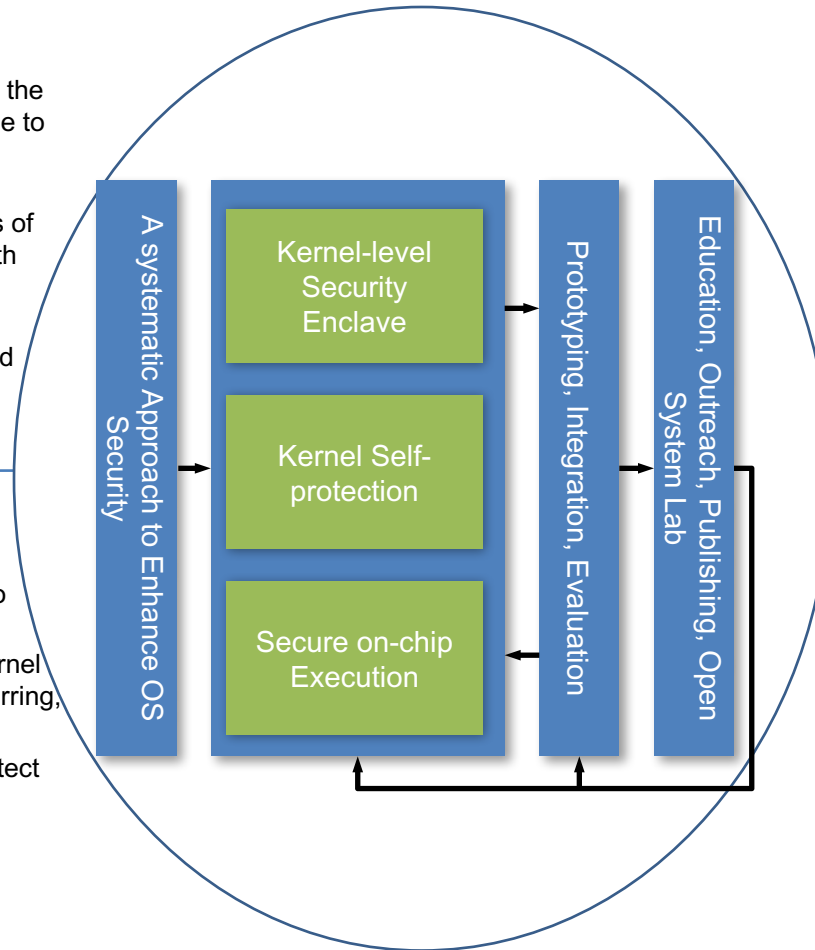# CAREER: Towards Trustworthy Operating Systems

**Challenge:**
- The kernel plays a critical role in the security of computer systems due to its high privilege.
- Modern kernels are hugely complicated with millions of lines of source code from developers with varying levels of skills.
- An increasing number of vulnerabilities are discovered and exploited in the kernel.

**Solution:**
- A generic kernel-level enclave to protect security mechanisms
- Enable self-protection for the kernel with kernel CFI, kernel binary stirring, and data-type integrity
- Secure on-chip execution to protect key data from cold-boot attacks



A systematic Approach to Enhance OS Security

- Kernel-level Security Enclave
- Kernel Self-protection
- Secure on-chip Execution

Prototyping, Integration, Evaluation

Education, Outreach, Publishing, Open System Lab

**Scientific Impact:**
- Effectively protect security mechanisms from kernel-level malware
- Protect the kernel code integrity and investigate possible solutions to kernel data integrity
- Protect key data (e.g., cryptographic keys) from powerful cold-boot attacks.

**Broader Impact:**
- Fundamentally improve our defensive capability against malicious and stealthy kernel malware and powerful cold boot attacks.
- Build open system lab at FSU CS with Raspberry PI-based projects (e.g., xv6 for PI)
- Continue to work with minority and female students, outreach to local high-school students

CNS #1453020
Zhi Wang
Florida State University