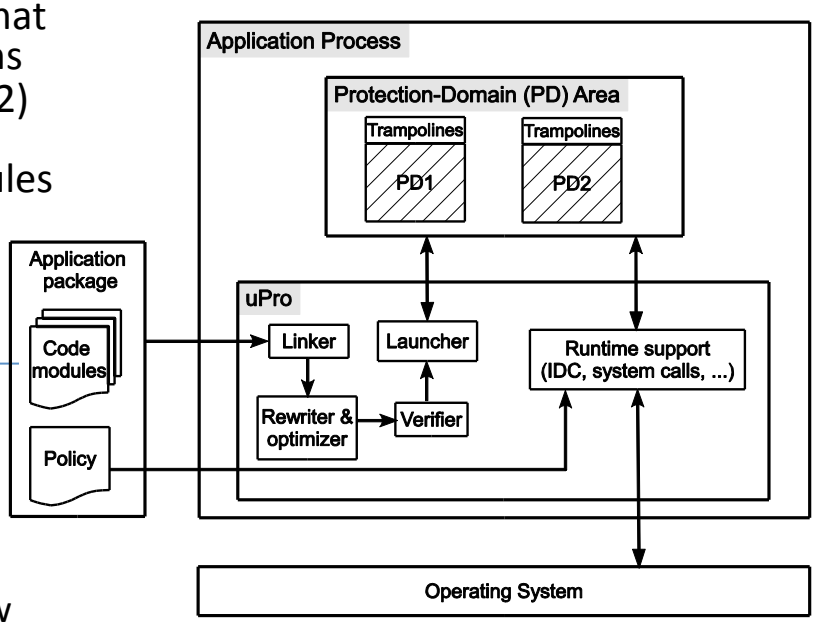
CAREER: User-Space Protection Domains for Compositional Information Security

Gang Tan, Pennsylvania State University

Challenge:

Design a privilege separation framework that (1) partitions applications into multiple modules, (2) enforces lightweight separation among modules (3) provides rigorous reasoning about the partitioned application



Solution:

- Lightweight isolation based on Software-based Fault Isolation (SFI) and Control-Flow Integrity (CFI)
- Automatic program partitioning that supports general programming (pointers, e.g.)

Scientific Impact:

- Provide developers an easy-to-use application partitioning framework
- Novel SFI/CFI systems with small overheads (~5%)

Broader Impact:

- Open sourced SFI/CFI implementation: https://github.com/mcfi/MCFI
- In collaboration with Google Research
- Hosted high-school teacher workshop on security and privacy
- Multiple REU participants

CCF-1624124, Pennsylvania State University, Gang Tan, gtan@cse.psu.edu