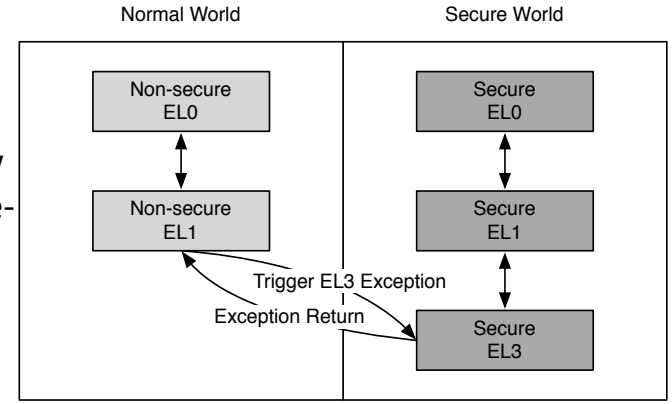
SaTC: CORE: Small: Collaborative: Hardware-assisted Plausibly Deniable System for Mobile Devices

WAYNE STATE UNIVERSITY

Michigan Tech

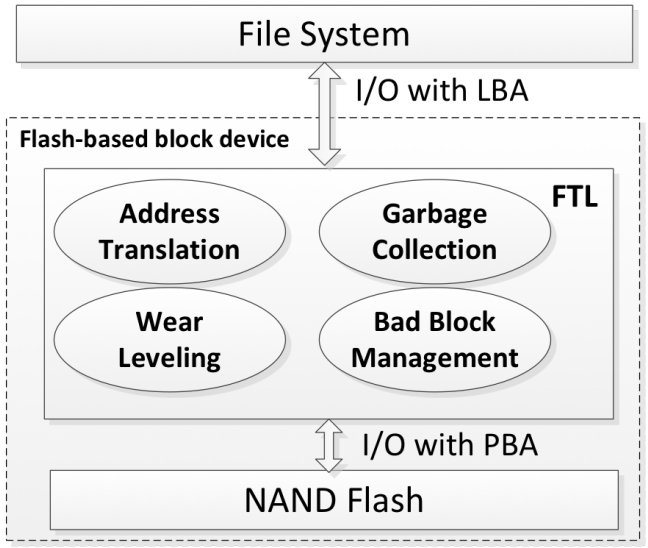
Challenge:

- The existing PDE systems for mobile devices are built at the block layer and suffer from raw flash snapshot attacks and side-channel leakages leading to deniability compromises



Solution:

- Discovered various deniability compromises in the FTL and designed novel techniques to eliminate them
- Strong isolation and fast mode switching via TrustZone
- Integrated FTL and TrustZone in a unique platform



Scientific Impact:

- Efficient (low-overhead) and effective (high deniability) hardware-assisted solution that leverages exiting hardware features such as flash translation layer (FTL) firmware and ARM TrustZone

Broader Impact and Broader Participation:

- PDE systems in mobile devices can deny existence of sensitive data
- Involved multiple graduate/undergraduate students into the project in WSU and MTU
- Won 2022 Michigan Collegiate Cyber Defense Network (3rd Place)
- Incorporated the project into graduate courses, cybersecurity reading group, K12 summer program for females in MTU

NSF CNS-1928331

Wayne State University, Weisong Shi (weisong@wayne.edu)

NSF CNS-1928349

Michigan Technological University, Bo Chen (bchen@mtu.edu)