SaTC: CORE: Small: Selective Data Protection against Data-oriented and Transient Execution Attacks

Challenge

- Memory disclosure vulnerabilities are becoming an important threat
- The threat of data leakage has been exacerbated by transient execution attacks, which leak data through microarchitectural side effects
- Existing isolation and sandboxing technologies are not adequate for preventing data leakage through transient execution attacks

Solution

- Design principled selective data protection techniques based on in-memory data encryption
- Enable developers to protect sensitive data (e.g., private keys) with minimal manual effort
- Maintain compatibility with complex, large-scale, real-world applications

Award Number: 2104148 (2021–2024) | Stony Brook University

Michalis Polychronakis (mikepo@cs.stonybrook.edu)

Scientific Impact

- Elevating sensitive data protection as a core language feature will enable developers to effortlessly protect in-memory data they deem critical
- Combination of static pointer analysis with scoped dynamic data flow tracking to minimize the heavyweight instrumentation required for keeping sensitive data encrypted in memory
- Selectively increasing the sensitivity of pointer analysis will improve overall analysis precision for large and complex applications

Broader Impact and Broader Participation

- Improve the state of the art in defenses against data-oriented and transient execution attacks
- Software prototypes readily applicable on third-party applications for both end users and researchers
- Participation and outreach programs through Stony Brook's Center for Inclusive Education (CIE) for undergraduate and graduate students, and Institute for STEM Education (I-STEM) for high school students