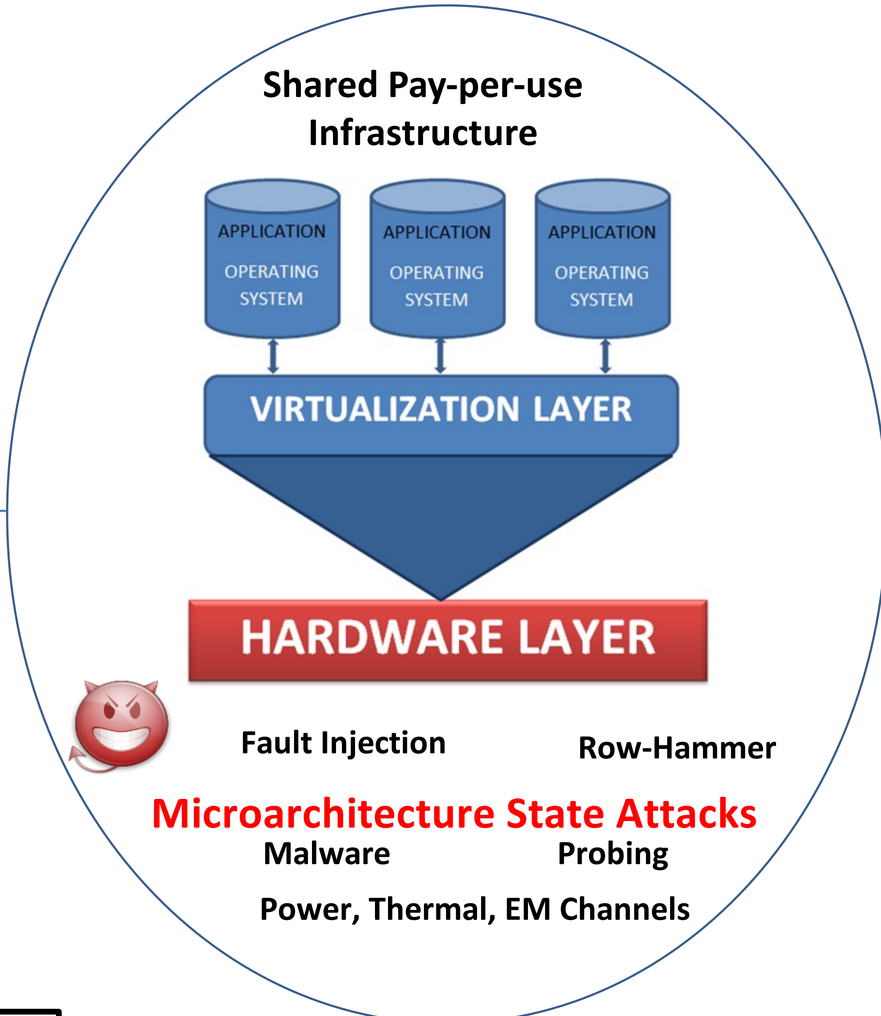
SaTC: CORE: Small: A Secure Processor that Exploits Multicore Parallelism while Protecting Against Microarchitecture State Attacks

Challenge:

- Highly virtualized systems share hardware resources for efficiency, but expose user private data during execution
- Today's secure processor technology vulnerable to threats such as malicious software exploiting timing variations in shared hardware resources to leak user sensitive data

Solution:

- Enable privacy-aware secure processor with ***strong hardware isolation*** technology that guarantees no process infers anything private from another process using shared hardware resources as a timing side-channel



Scientific Impact:

- Enhance ***confidential computing platforms*** (Intel TDX, AMD SEV, Arm CCA etc.) with novel methods for strong security and isolation guarantees at the processor system hardware level
- Develop spatial and temporal hardware isolation technologies that allow next generation secure multicore processors to execute code that keeps its internal computations private

Broader Impact and Broader Participation:

- Lead REU Site on Trustable Embedded Systems Security Research – 10-week summer opportunities for REU students to work on security topics, such as biobots, biometrics, voter systems, secure processors
- Collaborations with semiconductor companies, Arm, AMD, Qualcomm, NXP
- Transition project outcomes to industry via Semiconductor Research Corporation (SRC) collaborations
- Incorporated secure processor technology modules in undergraduate and graduate coursework
- Lead (General Chair) a new 2nd IEEE International Symposium on Secure and Private Execution Environment Design, SEED 2022 – https://seed-symposium.org

CNS-1929261

Omer Khan (Principal Investigator) -- khan@uconn.edu

University of Connecticut, Storrs, CT USA