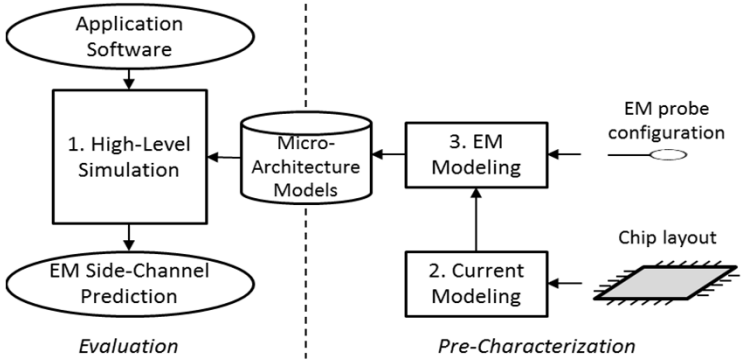
THE UNIVERSITY OF TEXAS AT AUSTIN
DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING
UT ECE

Simulation-Based Analysis of EM Side Channels in Embedded Systems: From Software to Fields

Challenge:

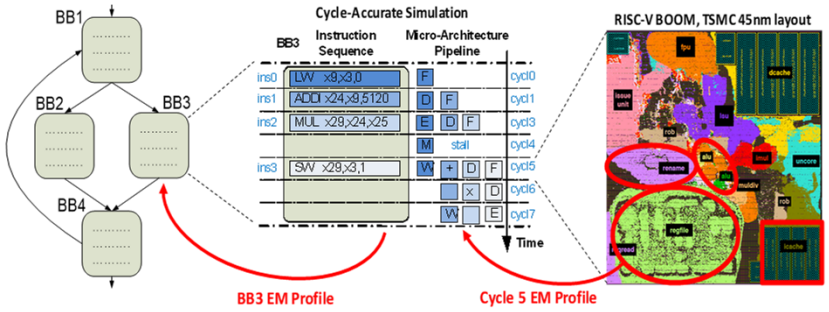
- EM leakage through software activity in embedded systems
- Currently, only lab-based characterization possible
- Requires expertise that a typical software engineer lacks



Pre-characterized EM macro-models are composable, allowing on-the-fly prediction of EM fields for application software.

Solution:

- Will develop tools to model EM side channels
- Via tracking of spatio-temporal EM fields from circuits to micro-architectures to software



Hierarchical macromodeling: Software is compiled into basic blocks (BBs) of instruction sequences. Spatio-temporal component-level EM profiles are composed into cycle-by-cycle and block-by-block profiles of software executing on the processor.

Scientific Impact:

- Improved system-level defenses against malware;
- Leakage reduction via HW/SW co-design at compiler/μArch levels

Broader Impact:

- Results will allow new design methods for embedded system security and privacy
- Extensive programs in undergraduate and K-12 outreach and cybersecurity training in collaboration with Texas Advanced Computing Center and NSF REUs

M. Orshansky, A. Gerstlauer, A. Yilmaz, University of Texas at Austin, Award #1901446, 2019-2023