TWC: Medium: Automating Countermeasures and Security Evaluation against Software Side-channel Attacks

Challenge:

- Automatically identify side-channel leakage
- Automatic and effective countermeasures
- Security verification

Leaky software

Masking
Shuffling
Randomization

Protected code

Scientific Impact:

- Leakage metrics
- Side-channel security aware compiler
- Security guarantee and proof

Solution:

- Early leakage detection
- A compile-time and run-time framework of software transformation to resist against attacks
- Rigorous security assessment and verification throughout

Broader Impact:

- Security-by-design and verifiable secure crypto engine
- Synergy among statistics, formal methods, and system security
- Automation tools for public

CNS1563697, Northeastern University,
Yunsi Fei, Aidong Adam Ding, Thomas Wahl
{y.fei,a.ding,t.wahl}@northeastern.edu