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

Multi-level: source-code, compiler, binary instrumentation

Multi-threats: power analysis, memory-based attacks

Multi-principles: randomization, shuffling, masking

Protected code

Scientific Impact:

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

Solution:

- An versatile early leakage measure - ILA
- Multi-level countermeasures against multiple leakage
  - Source code transformation against memory side-channel attacks
  - A leakage-aware compiler for threshold-implementation against power analysis
  - A framework of binary analysis to localize transition-based leakage and mitigation
- 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
http://tescase.coe.neu.edu