Practical Experiences Applying TVLA In Conformance Testing

The TVLA Ideal

The Test Vector Leakage Assessment (TVLA) approach to side-channel testing is proposed as similar in concept to CAVP program operations

- Standardized
    - Reproducible
    - Prescribed methods
    - Controlled test vector suite with updates
- Time bounded
- Feasible for 3rd party conformance testing

Laboratory Skill Set

TVLA requires tester to have a more technical skill set

- Signal exploration and isolation
  - Signal exploration is the art of finding the signal of interest
  - Signal isolation is the art of “cleaning up” the signal of interest for best results in the correlation processes to come
  - Tester background in RF and signal processing is a necessity
- MATLAB (or similar) skills to manipulate datasets
- Detailed algorithm implementation awareness is a must
  - An appropriate math background is helpful
- Expect longer training
- Extensive practice is necessary to become proficient
- A standardized, reproducible regulatory accreditation process is challenging

Interaction with Vendors

Labs should expect to educate vendors on the goals, process and conclusions of the process

- In many cases, vendors will be unsure of existing countermeasures or have the ability to control them
- Instrumentation of the system under test is required
  - CAVP permits an honor system approach to algorithm testing …
  - The honor system approach to trace capture is unworkable for TVLA
- Interacting with vendors about unsatisfactory findings

False Negatives

The TVLA process is more susceptible to false positive results

- A CAVP process fault is likelier to result in a false negative
- The TVLA process must assure a passing result is valid
  - Demonstrating leakage impact of enabling / disabling countermeasures provides good confidence
  - Demonstrating leakage in I/O provides some confidence
- Signal exploration failures may be a tester skill problem
- Poor signal cleanup can yield misleading results

Interpretation of results

A TVLA pass or fail conclusion out of context is too simplistic

- The vendor may need to disable effective countermeasures to allow the TVLA testing process
- A consistent leakage threshold may be hard to agree on
  - Key lifecycle and the nature of the crypto functions are factors
  - Scoring systems are helpful to provide context
- A periodic dialog between industry, regulators and labs to establish ground rules for interpretation will help
- Drawing conclusions from simple leakage tests
  - *Fixed vs varying* tests should spot leakage
  - More specific tests shed additional light, but have cost, time and resource implications, and require update as methods evolve

On the good news front …

The comparison to CAVS is not completely apt … but TVLA is a good approach for compliance scenarios

- Straightforward and constrained process
- Test vectors are predetermined, standardized & maintained
- Inclusion of fixed vs varying is a good sanity check
  - A broad approach to uncovering leakage

TVLA for compliance scenarios is a good direction … *and* …

- TVLA needs greater definition and support from the community
  - Community: industry, regulators and labs
- Labs need to prepare tooling and training for a non-trivial new task

Thank you!

www.infogard.com