Test Vector Leakage Assessment (TVLA) for Side Channel Analysis in Conformance Testing Scenario (A16a)

Gilbert Goodwill

November 5, 2015

Rambus

Test Vector Leakage Assessment (TVLA)

- Side-channel testing for standardized testing applications
- Instead of traditional evaluation attack scenario requiring
  - Algorithm-specific knowledge
  - Up to date with latest attacks
  - Trial and error until success or allotted time/effort is exhausted…

Test Vector Leakage Assessment

- Use specified test vectors
  - Known key, data
  - Encompass cipher-specific knowledge to trigger different possible leakages
- t-Test on known quantities for leakage measurement
  - Pass/fail test on leakage levels for exploitable information
  - Tests whether there is a statistically significant difference between means
  - Thresholds set at 99.999% confidence (and higher)

Algorithms and Tests

- AES-128, -192, -256
  - S-box output; round output; round input ⊕ output, S-box input ⊕ output
  - Fixed-vs.-varying, semi-fixed-vs.-varying
- DES, TDES
  - Same as intermediates AES
- SHA256, HMAC-SHA256
  - Round output, message schedule, t1, t2, round input ⊕ output
  - Fixed-vs.-varying
- Public key: RSA, ECC
  - Semi-fixed-vs-varying

Test Vector Leakage Assessment (TVLA)

- Signal finding is required
  - Skill must be developed in testing laboratories
  - Once developed is applicable across ciphers
- Confirm successful signal isolation
  - Using leakage of non-sensitive quantities such as input and/or output
  - Absence of signal does not mean absence of leakage

Attack potential factors

- Signal isolation may require
  - Expertise
  - Knowledge of device
  - Equipment, parts, etc.
- Tests target exploitable intermediates and general leakage
  - Exploitable intermediates have direct parity with attack number of traces
  - Non-specific (fixed-vs.-varying) tests combine leaks together
    - Show leakage failures earlier than an attack may be possible