Test Vector Leakage Assessment (TVLA) methodology in practice
(Extended Abstract)
Authors: Jeremy Cooper, Elke DeMulder, Gilbert Goodwill, Joshua Jaffe, Gary Kenworthy and Pankaj Rohatgi, Cryptography Research Inc.

Many security standards require cryptographic devices and modules to resist side-channel attacks such as Timing Analysis as well as Simple and Differential Power/Electromagnetic Analysis. These requirements have also been included in the draft FIPS 140-3 standard [1]. However, existing security certification standards mandating side-channel resistance, such as Common Criterion, require an evaluation style testing approach to verify compliance. Such evaluation style testing approaches are not suitable for a conformance style testing program such as CMVP, and effective, yet cost-efficient, conformance style testing for side-channel resistance has been seen as a challenge.

At the NIST sponsored NIAT workshop in 2011, a promising new approach for performing conformance style testing for side-channel resistance was presented for the AES and RSA algorithms [2,3]. The approach was based on measuring power consumption from devices while performing cryptographic operations with a pre-specified set of input test vectors and then performing a set of pre-specified statistical tests on the collected power measurements. These statistical tests yield confidence scores, using which clear fail/pass criterion can be established. These papers also presented preliminary experimental results on different devices to establish that these tests could detect sensitive information leakage within the power side-channel, within a reasonably short amount of time and without requiring test operators to become skilled in performing the latest side-channel attacks.

In this paper and presentation, we will describe our experiences in using and enhancing this methodology which we have renamed as “Test Vector Leakage Assessment”, as part of our analysis flow for performing side-channel assessment of tens of cryptographic devices, as well as part of our design flow for creating side-channel resistant implementations over the past two years.

Our experience has confirmed that this methodology is a reliable, quick and easy test for detecting potential side-channel problems with devices. Often our analysis requires us to perform key extraction attacks and the TVLA testing, which focuses on detecting sensitive information leakage, is one to two orders of magnitude faster in detecting a leakage problem with a device than performing a full key extraction attack. TVLA based testing methodology also lends itself to real-time testing: the statistical tests can be performed as the measurements are being collected. In the full paper and presentation, we will describe examples and comparison of TVLA testing time vs. key extraction attack time, and will also demonstrate our system performing real time TVLA testing on an AES image on an FPGA.

Our experience has shown that the non-specific tests of leakage presented in [2,3], i.e., those which compare measurements when the device is repeatedly performing some fixed operation vs. measurements when the device is performing operations where randomly generated inputs, to be the
most powerful. These tests cover a wide variety of leakages and can often detect problems with a device with an order of magnitude fewer measurement traces than tests targeting specific classes of leakage. Non-specific tests for AES and RSA have therefore become the first analysis that we perform while data is being collected from a device, so that problems can be detected early in the process. Based on our experience with a variety of platforms, including mobile devices, we have further enhanced and optimized these non-specific tests in two different ways.

The first enhancement dramatically speeds up the data collection and testing process for AES, by one or more orders of magnitude. It has been found to be most useful for mobile platforms and for designer’s seeking quick feedback on their DPA-resistant design in software or on an FPGA. The improved approach works as follows: The device or implementation is configured to perform bulk AES encryption, with either the fixed data or on random data. For AES-CBC mode, the input data is adjusted so that the input to the AES operation after the chaining is always the same as the specified test vector, but the random data could be arbitrary. With this approach, a single data collect from the sampling oscilloscope can yield several hundred/thousands of AES operations performed during a single bulk operation. Software is then used to split the single trace into the individual AES encryption segments for performing the TVLA testing. With this approach it is possible to collect many orders of magnitude more traces in the same amount of data collect time and analysis involving millions of AES operations, e.g., to validate a masked AES implementation on an FPGA, can be carried out in a matter of days. This approach also works quite well for mobile and software platforms where interrupts or other interference can seriously degrade the parsing of the individual AESs encryption segment in the signal. For the non-specific, fixed vs. random test, there is no need to precisely map which AES signal corresponds to which random (or fixed block) in the presence of these interrupts and interference! The test can be done using only those AES signal segments which are clearly identified to be from either the fixed set or from the random set. In contrast, the non-specific tests or attacks require substantial signal processing to identify which signal segment corresponds to which encryption operation, and this can easily take an order of magnitude extra effort and time. In the full paper and presentation, we will provide details and results for such AES testing on mobile platforms and hardware based AES implementations.

The second enhancement to the non-specific, fixed vs. random testing is targeted to devices where there is substantial usage of timing noise and amplitude noise countermeasures, and the precise start and end of the AES operations cannot be determined from the signal. In such cases, it is reasonable to expect the vendor to provide a trigger at the initiation of the AES command or when the timing/amplitude noise generation is started during the AES command processing. The fixed vs. random test however, requires the test operator to ignore the start and end of AES and focus only on the middle third of the operation, as the fixed input and output processing from the fixed data set can have a different side-channel profile from the processing of random inputs and outputs without creating a key extraction vulnerability. However, with timing/amplitude noise, the middle third of the AES cannot be determined from the traces or from the trigger signal. To handle these and other cases, we have modified the fixed vs. random test to create semi-fixed set of test vectors for AES where the input and outputs are statistically random, but significant parts of one or more interior rounds of AES is kept fixed.
These semi-fixed test vectors can be used in place of the fixed test vector for the non-specific fixed vs. random set, without impacting the effectiveness of the test or identifying the middle third of AES. Details of this approach and the recommended semi-fixed test vectors will be provided in the full paper/presentation.

References