Side-Channel Analysis Assignment 3

Hardware Security – Spring 2019

April 18, 2019

1 Template Attacks

The purpose of this exercise is to use templates that can distinguish two operations O_0 and O_1. Operation O_0 manipulates the value 0 and operation O_1 manipulates the value 1, i.e. the context corresponds to a cryptographic implementation with keys 0 and 1.

In order to build templates, you need to create your models based on training datasets for operations O_0 and O_1. The validity of the built models can then be tested using the testing datasets for O_0 and O_1 respectively. The datasets are available here (7k traces for each training dataset and 3k traces for each testing dataset. Each set has 1301 sample points.):
`https://mega.nz/#!C59TVboT!CKlib1wKOPbgyvBsAbzlk5J2ENehkGW2W-5YyukbtlY`

1. Build reduced templates for operations O_0 and O_1 using the training datasets. Subsequently, compute the misclassification rate for each operation, using the testing datasets. In other words, compute the percentage of each testing dataset that is matched to the incorrect template, i.e. $no\_mismatches/TestSetSize$.

2. Build univariate templates for operations O_0 and O_1 using a single sample of the training datasets. You can choose the sample (a.k.a. Point Of Interest – POI) using the absolute difference of means heuristic for POI selection. Compute the theoretical false positive and false negative w.r.t. to the two estimated univariate normal distributions. Compute also the misclassification rate for each operation using the corresponding testing sets.

3. Build multivariate templates for O_0 and O_1 using principal component analysis. Perform the following procedure (also available here: `https://www.iacr.org/archive/ches2006/01/01.pdf`).

   (a) Compute the mean of the two operations $\bar{\mathbf{t}} = 1/2 * \sum_{k=0}^{1} \mathbf{t}_k$, where $\mathbf{t}_k$ is the mean of operation O_k.

   (b) Compute $B = 1/2 * \sum_{k=0}^{1} (\mathbf{t}_k - \bar{\mathbf{t}}) * (\mathbf{t}_k - \bar{\mathbf{t}})^T$. The result is a 1301 x 1301 matrix.

(c) Perform the singular value decomposition of B, using $[U, S, V] = svd(B)$ in Matlab.

(d) Choose the number m of dimensions (principal components) that you want, i.e. perform $U_{reduced} = U(:, 1 : m)$. The size of $U_{reduces}$ is $1301 \times m$.

(e) Project all datasets ($testSet0, testSet1, trainSet0, trainSet1$) using $U_{reduced}$, i.e. perform matrix multiplication in order to produce a $7000 \times m$ and $3000 \times m$ matrices.

(f) Compute the mean vector and the covariance matrix from the projected training datasets, i.e. build the multivariate templates using Matlab $mean$ and cov.

(g) Compute the misclassification rate for the projected testing datasets. Set m experimentally to a value that minimizes the misclassification rate.