Finding Statistical Differences in Devices Through Leakage

Fall 2022

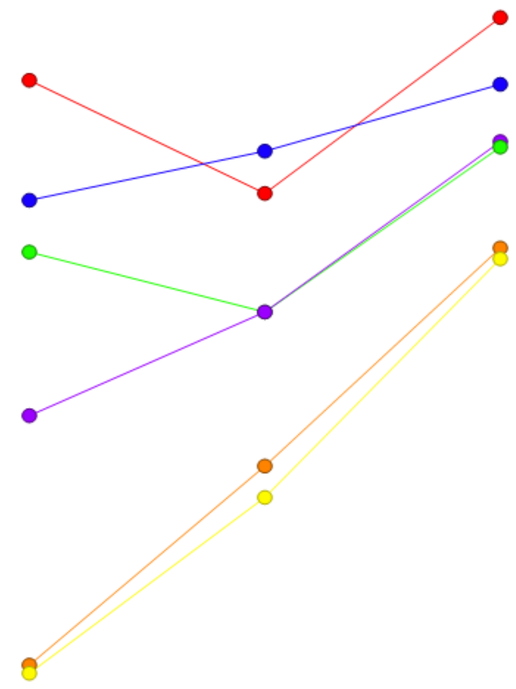
Testing for the Secret Key

Abstract

Statistical analysis methods for side-channel attacks are limited. Testing side channel is through Test Vector Leakage Assessment (TVLA). The importance of TVLA is to show whether side channel attacks can get data from the cryptographic device in question. The three major methods used currently are the Pearson Chi-square test, Pearson's correlation coefficient and Welch's t-test for testing differences of means.

Methods

Our methods will first involve generating a dataset from different devices. We will use this data to hypothesis test whether there is a difference in mean leakage between the different devices.



Preliminary Results

The current preliminary results are that the aforementioned statistical methods (Pearson Chi-square, Pearson's Correlation, and Welch's t-test) do find significance in determining leakage noise and the actual private key leakage.

Challenges & Future Work

The current challenge is finding a good place to start. An idea on future work, depending on results, would be that we could generalize what early differences in leakage each device has, and as such, we can determine how to implement further side-channel attacks to extract the secret key.

Advisor: Dr. Mike Borowczak

Group Members:

- Clay Carper (ccarper2@uwyo.edu)
- Stone Olguin (aolguin1@uwyo.edu)

University of Wyoming

CEDAR
Cybersecurity Education And Research Center

UW School of Computing | UW College of Engineering and Physical Sciences | UW College of Engineering and Physical Sciences Electrical Engineering and Computer Science | UW Cybersecurity Education and Research Center