Smartphone Side-Channel Attacks and Defenses: A Course Project

UNIT

Chuan Yue - February 19, 2019

Description

This set of Smartphone Side-Channel Attacks and Defenses curriculum materials are designed to help undergraduate and graduate students to deeply learn advanced motion sensor based side-channel attacks and defenses on smartphones. It consists of one unit (a course project) with five children modules (Lab 1 to Lab5):

A Course Project unit with five modules:

- Lab 1 Motion sensor data collection toolkit development
- Lab 2 Motion sensor data preprocessing
- Lab 3 Motion sensor data feature extraction
- Lab 4 Model training and evaluation
- Lab 5 Motion sensor data perturbation for defense

We designed the materials in a way that they can be flexibly used by an instructor to either assign a semester-long course project to students to comprehensively learn all the five aspects (related to the five labs) of the topic, or assign any of the five modules as an independent lab exercise for students to focus on learning one specific aspect of the topic.

Please read the Overall Instructor Manual CSM_NCCP_Smartphone_Side-Channel_Attacks_Defenses_Overall_Instructor_Manual.docx for more details about how you may want to use these curriculum materials.

evaluate and synthesize

Students will be able to construct tools to preprocess smartphone motion sensor data.

evaluate and synthesize

Students will be able to build tools to collect motion sensor data from smartphone users without any restriction.

evaluate and synthesize

Students will be able to design features for machine learning algorithms based on the preprocessed motion sensor data.

evaluate and synthesize

Students will be able to compose a research-paper style course project report.

evaluate and synthesize

Students will be able to create powerful side-channel attacks for compromising users' security and privacy by leveraging the collected data and machine learning techniques.

evaluate and synthesize

Students will be able to design defense techniques to protect against motion sensor based side-channel attacks.

Notes

Note that the solution manual and the solution materials are not uploaded to this platform based on the suggestion from Kaza, Siddharth (SKaza@towson.edu).

Please contact Dr. Chuan Yue (chuanyue@mines.edu) at the Colorado School of Mines for the solution manual and the solution materials.

The development of this module is sponsored by the NSA grant H98230-17-1-0403.