Motion sensor data perturbation for defense

MODULE

Chuan Yue - February 19, 2019

Description

Upon completion of this lab, students should be able to:

Interpret two representative data perturbation based defense techniques.

Assessed by the tasks and outputs specified in STEP 1.

Construct new datasets by applying two data perturbation based defense techniques.

Assessed by the tasks and outputs specified in STEP 2.

Create machine learning models with training, hyper-parameters tuning, and evaluation for performing input inference attacks using the newly constructed datasets.

Assessed by the tasks and outputs specified in STEP 3.

Create machine learning models for performing user fingerprinting attacks using the newly constructed datasets.

Assessed by the tasks and outputs specified in STEP 4.

Compare two data perturbation based defense techniques in terms of their effectiveness on reducing the attack accuracy.

Assessed by the tasks and outputs specified in STEPs 3 and 4.

Estimate the potential side-effects of two data perturbation based defense techniques.

Assessed by the tasks and outputs specified in STEP 5.

Propose new ideas to protect against motion sensor based side-channel attacks.

Assessed by the tasks and outputs specified in STEP 6.

Outcomes

evaluate and synthesize

Students will be able to create machine learning models with training, hyper-parameters tuning, and evaluation for performing user fingerprinting attacks using the newly constructed datasets.

evaluate and synthesize

Students will be able to estimate the potential side-effects of two data perturbation based defense techniques.

evaluate and synthesize

Students will be able to create machine learning models with training, hyper-parameters tuning, and evaluation for performing input inference attacks using the newly constructed datasets.

evaluate and synthesize

Students will be able to construct new datasets by applying two data perturbation based defense techniques.

evaluate and synthesize

Students will be able to compare two data perturbation based defense techniques in terms of their effectiveness on reducing the attack accuracy.

evaluate and synthesize

Students will be able to propose new ideas to protect against motion sensor based side-channel attacks.

remember and understand

Students will be able to interpret two representative data perturbation based defense techniques (reducing data sampling frequency and adding noises to the data).

Content

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.