smartphone Side-Channel Attacks and Defenses

**Overall instructor Manual**

**Course Project Development Institution:** Colorado School of Mines

**Course Project Manual Contributor**: Chuan Yue

# An Overall instructor Manual for Advanced Smartphone Side-Channel Attacks and Defenses

**Overview:**

Motion sensors such as accelerometers and gyroscopes are ubiquitously equipped in modern smartphones. They have enabled mobile apps to have richer functionality and better interactivity, but have also created many new opportunities especially powerful side-channels for attackers to compromise users' security and privacy. In particular, both input inference attacks and user fingerprinting attacks can be effective.

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.

**Guide for Using the Materials:**

If an instructor plans to use the materials to assign a semester-long course project to students to comprehensively learn ***all the five aspects of the topic***, the following files are related (the first three are for both the instructor and students, while the solution is for the instructor only):

* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_CourseProject\_Manual.docx
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_CourseProject\_Information.xlsx
* CSM\_MotionSensor\_Dataset.zip
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_CourseProject\_Solution.docx

If an instructor plans to use the materials to assign a lab exercise for students to focus on learning ***the motion sensor data collection toolkit development aspect of the topic***, the following files are related (the first two are for both the instructor and students, while the solution is for the instructor only):

* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module1\_Manual.docx
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module1\_Information.xlsx
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module1\_Solution.docx

If an instructor plans to use the materials to assign a lab exercise for students to focus on learning ***the motion sensor data preprocessing aspect of the topic***, the following files are related (the first three are for both the instructor and students, while the solution is for the instructor only):

* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module2\_Manual.docx
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module2\_Information.xlsx
* CSM\_MotionSensor\_Dataset.zip
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module2\_Solution.docx

If an instructor plans to use the materials to assign a lab exercise for students to focus on learning ***the motion sensor data feature extraction aspect of the topic***, the following files are related (the first three are for both the instructor and students, while the solution is for the instructor only):

* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module3\_Manual.docx
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module3\_Information.xlsx
* motion\_data.pkl
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module3\_Solution.docx

If an instructor plans to use the materials to assign a lab exercise for students to focus on learning ***the model training and evaluation aspect of the topic,*** the following files are related (the first three are for both the instructor and students, while the solution is for the instructor only):

* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module4\_Manual.docx
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module4\_Information.xlsx
* feature\_data.csv
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module4\_Solution.docx

If an instructor plans to use the materials to assign a lab exercise for students to focus on learning ***the motion sensor data perturbation for defense aspect of the topic***, the following files are related (the first four are for both the instructor and students, while the solution is for the instructor only):

* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module5\_Manual.docx
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module5\_Information.xlsx
* CSM\_MotionSensor\_Dataset.zip
* motion\_data.pkl
* CSM\_NCCP\_Smartphone\_Side-Channel\_Attacks\_Defenses\_Module5\_Solution.docx

**Solution Manual and Materials:**

We developed a complete set of solution manuals (those \*\*\*\_Solution.docx files mentioned above) and solution materials (including the data collection toolkit and tools or source code) for the unit (course project) and the five labs. They were not uploaded to the CLARK system due to its lack of access control to students and also based on the suggestion from Kaza, Siddharth (SKaza@towson.edu).

Please contact Dr. Chuan Yue (chuanyue@mines.edu) at the Colorado School of Mines or NSA NCCP program directors for the solution manuals and the solution materials.

**Course Project or Lab Environment:**

Either Linux, Mac, or Windows systems will be appropriate. In more details, the operating systems and software packages that we used for developing these materials (including solution materials) are listed below for your reference; however, higher versions of OSes and software packages should also work:

* OS version: Ubuntu 14.04, or macOS 10.12.6
* Python version: 3.5
* Python packages: default version of pickle, sklearn, numpy, and csv
* PHP: version 5 (note that this is needed only for Lab 1)

**Learning Setting:**

The unit (course project) and the five labs are for students to complete outside the classroom, so they can be used in either face to face or online courses.

**Prerequisites:**

Java or Python Programming, Basic Cybersecurity and Machine Learning knowledge and skills, Linux or Windows Systems, Computer Networks.

**Level of Instruction:**

Senior undergraduate students or graduate students in CS or related STEM programs. The materials should be further simplified if they will be used for freshmen, sophomores, or none-CS major students.

**Related Research Papers:**

The following four research papers can be the references to instructors and students who are using this set of curriculum materials:

* Sensor-based Mobile Web Fingerprinting and Cross-site Input Inference Attacks (position paper). By Chuan Yue. In proceedings of the IEEE Workshop on Mobile Security Technologies (MoST), 2016.
* Cross-site Input Inference Attacks on Mobile Web Users (short paper). By Rui Zhao, Chuan Yue, and Qi Han. In proceedings of the International Conference on Security and Privacy in Communication Networks (SecureComm), 2017.
* Effective Mobile Web User Fingerprinting via Motion Sensors. By Zhiju Yang, Rui Zhao, and Chuan Yue. In proceedings of the IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2018.
* Sensor-based Mobile Web Cross-site Input Inference Attacks and Defenses. By Rui Zhao, Chuan Yue, and Qi Han. In IEEE Transactions on Information Forensics and Security (TIFS), 2019.

Instructors and students are welcome (but not necessary) to glance those papers about the nature and some details about the input inference and user fingerprinting attacks. However, the dataset used in this set of curriculum materials is newly collected and is completely different from the dataset used in those four research papers. Meanwhile, this set of curriculum materials are newly designed for education and student training purposes; these labs are significantly different and much simpler than what we did in those research papers. Instructors and students can leverage many other references and links provided in these papers for them to better use this set of curriculum materials. If you cannot find these papers online, please contact Dr. Chuan Yue to obtain an author’s copy.

**Everything Else:**

Please check the detailed manuals or contact Dr. Chuan Yue (chuanyue@mines.edu) at the Colorado School of Mines or NSA NCCP program directors.