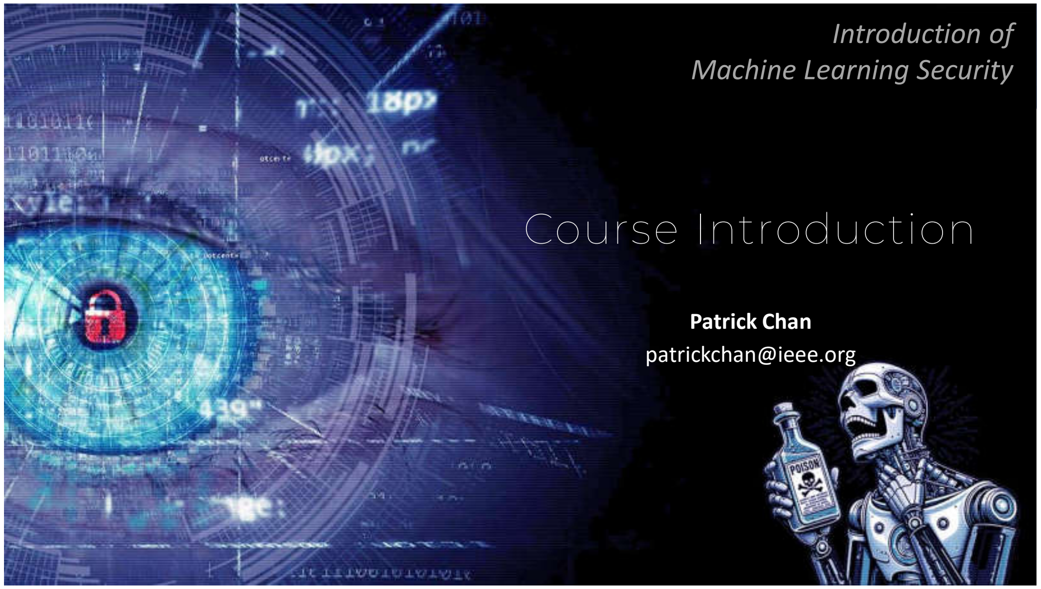


Introduction of
Machine Learning Security

Course Introduction

Patrick Chan
patrickchan@ieee.org

Dr. Patrick Chan

- Associate Professor & Deputy Dean,
  Shien-Ming Wu School of Intelligent Engineering

- E-Mail: patrickchan@scut.edu.cn
- QQ: 804273141
- WeChat: p-a-t-r-i-c-k
- Office: D1-b505

Course Information

- **One-semester** course
- **1** Credit
- **16** Teaching Hours (All Lectures)
- Venue: **F3-b311**
- Date & Time

	Mon	**Tue**
Week 13	08:50 – 11:30	08:50 – 11:30
Week 14	08:50 – 11:30	08:50 – 10:25
Week 15	08:50 – 11:30	08:50 – 10:25

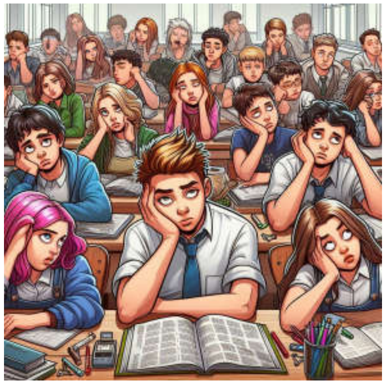
Course Information

- **Mode of Study**
  - Lecture
  - Assignment

- **Grading**

Participation	20%
Assignment (Programming is needed)	80%

Total	100%



ALERT! Dangerous!

- Prerequisites for Assignments:
  - Machine Learning
  - Deep Learning
  - Programming in Python
    - Pytorch
- Highly rely on yourself
- You may fail if you cannot do so!

Website

- Course Material can be download here

  https://teaching.mlclab.org/MLSec/index.htm
- You can download
  the lecture notes after lessons

References

- **Machine Learning Security (main reference)**
  https://github.com/unica-mlsec
- **Adversarial Robustness - Theory and Practice**
  https://adversarial-ml-tutorial.org/

Cheating

- It is a **very important part** of your university **education**
- You should **do your own job**
  (e.g. assignments and test/examination paper)
- **Simple Rule:**
  - Never use someone else's codes
  - Do not let someone copy your work
- **If cheating is found**
  - **Zero mark (both)**
  - **Report to the School and the University**

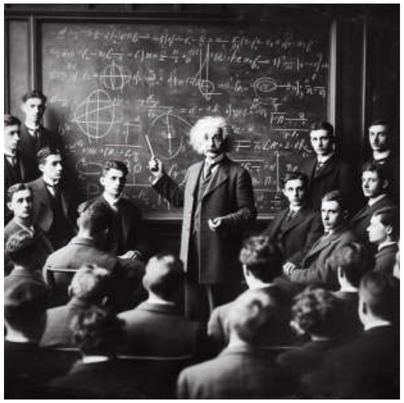
Goal

- After the course, you should able to
  - Understand the security vulnerability of ML applications
  - Know how to improve their security
- Aim
  - Introduce the basic idea of ML security
  - Basic ideas, pros and cons of attacks and theirs countermeasures
  - Understand the formulation of models (Mathematics)
- NOT Aim
  - Introduce all detail and implementation

My Teaching Philosophy

- I never teach my pupils;
  I only attempt to provide the
  conditions in which they can learn

  Albert Einstein



- Advices
  - **Enjoy each lesson**
  - **Interaction!**
  - **Think more**
  - **Ask questions**
  - **Smile ☺** ***(even you fail)***