Fun with Information Engineering and Security Summer 2024

Day 1 (Jul-31, Wed)

Department of Information Engineering

香港中文大學
The Chinese University of Hong Kong

Information

- Instructor: Sze Yiu, CHAU (SHB 707)
  sychau@ie.cuhk.edu.hk

- Teaching Assistants:

  - Angela Mak

  - Tony Tu

A little bit about myself

- Joined CUHK IE in 2020 Jan

- PhD in CS from Purdue University

- Post-doc researcher @ CMU CyLab

- Interests: Testing, analyzing and breaking protocol implementations + deployments

  ▫ 2 of my previous students got USD ~$20k in total from Google for finding flaws in Android & Chrome OS

❶ University MTR Station (Northern Exit)>

1. Fong Yun Wah Hall > 2. Yasumoto International Academic Park (escalator)> 3. Wu Ho Man Yuen Building (escalator) > 4. Wen Chih Tang > 5. Lee Shu Pui Tang > 6. Madam S.H. Ho Hall >
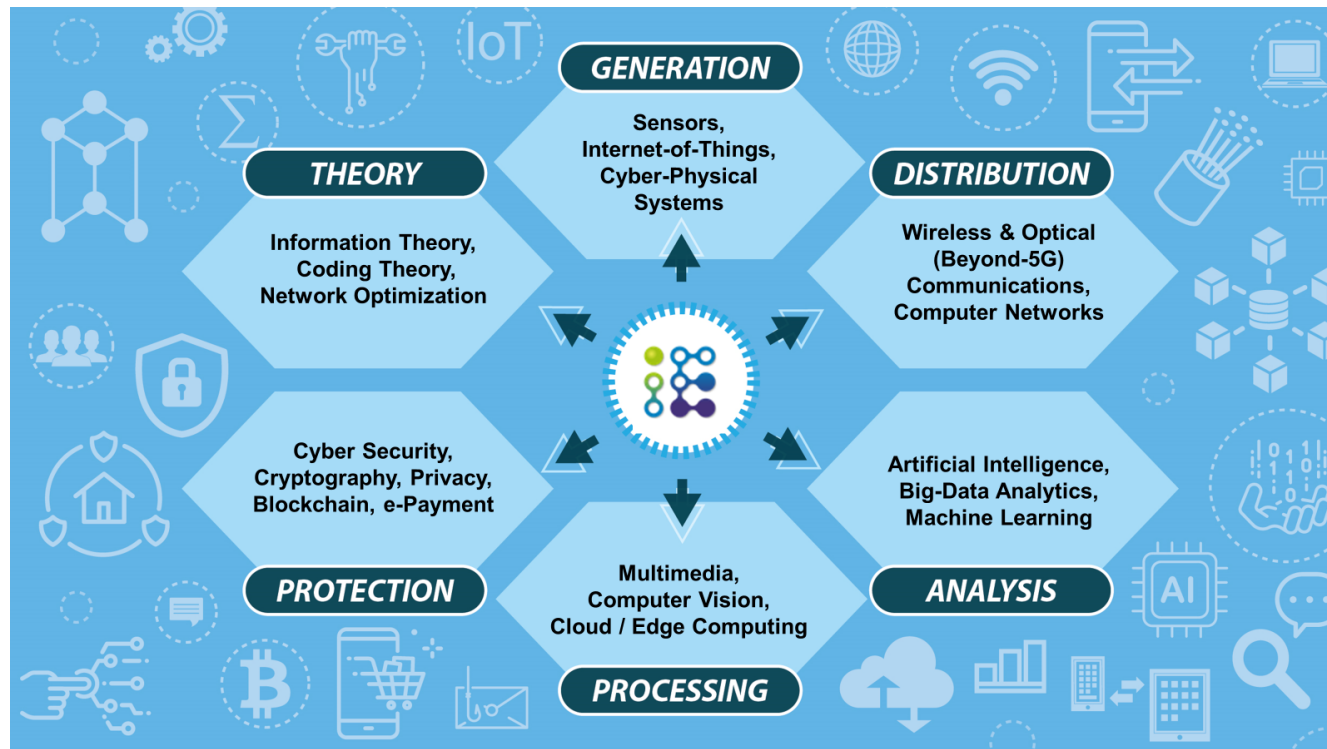
• To Central Campus

7. Nursery Path > 8. William M.W. Mong Engineering Building (lift to 10/F)

Fun stuff to see/read

Online resources

- Hacking Enterprise Wi-Fi and VPNs

So what is IE?

- We will focus on the basics of processing + protection

Workshop Information - Web Platforms

- Homepage

  - **https://staff.ie.cuhk.edu.hk/~sychau/summer24/**

  - get slides + lab sheets

- Virtual lab

  - **https://iesummerworkshop.github.io**

  - interactive programming environments + challenges

  - (credit goes to the TAs)

  - **PLEASE USE GOOGLE CHROME**

Workshop Information - Computers

- No need to bring/use your own computers
  - (you can, but not necessary)
- We will use the computers here, with guest accounts

  - Username: cuieg-sw@cuhk.edu.hk
  - Password: ab1234!!@

Workshop Information - Web Platforms

- <u>Homepage</u>

  - **https://staff.ie.cuhk.edu.hk/~sychau/summer24/**

  - get slides + lab manuals

- <u>Virtual lab</u>

  - **https://iesummerworkshop.github.io**

  - interactive programming environments + challenges

  - (credit goes to the TAs)

  - **PLEASE USE GOOGLE CHROME**

Workshop Information - Certs & Prizes

- Certs of attendance will be given to those who attend all 6 sessions (3 days)

- Additionally, there are small prizes for solving challenges

  - IE flash drives and/or snacks

    - PLEASE LET US KNOW IF YOU HAVE **FOOD ALLERGIES**

      - if you don't know whether you have food allergies, better not take the snacks

Workshop Information - Schedule

- **https://staff.ie.cuhk.edu.hk/~sychau/summer24/**

Topics and schedule

Date & time	Topics
Jul 31 (Wed) 14:00 - 16:00	Basic Python
Jul 31 (Wed) 16:00 - 16:15	*short break*
Jul 31 (Wed) 16:15 - 18:15	Information encoding & representation
Aug 01 (Thr) 14:00 - 16:00	Fun with ciphers I
Aug 01 (Thr) 16:00 - 16:15	*short break*
Aug 01 (Thr) 16:15 - 18:15	Fun with ciphers II
Aug 02 (Fri) 14:00 - 16:00	Input validation & Web security
Aug 02 (Fri) 16:00 - 16:15	*short break*
Aug 02 (Fri) 16:15 - 18:15	Input validation & System exploits

Workshop Information - Participants

- We have a very diverse set of participants

  - Most are senior year students (secondary schools)

  - Quite a few junior year students (secondary schools)

  - Some CUHK UGs (?)

Workshop Information - Participants

- All are welcome, but
  - Some might find the content a bit challenging
    - That's OK, just raise your hand and ask for help
      - The TAs and I will help you
  - Some might find the content a bit too easy
    - That's OK too, bear with us, and feel free to explore the challenges ahead of schedule on your own

Part 1 – Basic Python Programming

- Programming: instruct computers to do things

- Python is quite useful these days

  - Relatively easy to write/maintain

  - Good for prototyping (esp. attacks)

  - Also heavily used in data analytics & AI

- Let's go to the lab manual

  - **https://staff.ie.cuhk.edu.hk/~sychau/summer24/**

Part 2 - Encoding

- This can allow you to use things that you already have to represent **numeric values**

  - E.g., you might have voltage (high, low)

    - Intuitively, this can represent 1 bit (<u>1, 0</u> in binary)

    - (this is often how we make analog signal "<u>digital</u>")

Part 2 - Encoding

- This can allow you to use things that you already have to represent **numeric values**

  - E.g., you might have (human) readable text (e.g., sending messages via SMS or emails)

    - Then you can use that to represent binary files (e.g., images)

      - Not all files are "texts", try to open an image file with notepad, it's unintelligible

      - But we can treat the binary file as a (big) number, then choose a "base" represent it with "digits" in text

Part 2 - Encoding

Typical character sets for "digits" in different bases

- Base 2 (1 bit):
  '0' '1'

- Base 10:
  '0' '1' '2' '3' '4' '5' '6' '7' '8' '9'

- Base 16 (4 bits):
  '0' '1' '2' '3' '4' '5' '6' '7' '8' '9' 'A' 'B' 'C' 'D' 'E' 'F'

- Base 64 (6 bits):
  'A' to 'Z' 'a' to 'z' '0' to '9' '+' '/'

Part 2 - Encoding

Typical character sets for "digits" in different bases

- ASCII can be seen as a special "Base 256"
  - 8 bits per character
  - The mapping from "value" to "digit" (character) can be found in the ASCII table

Part 2 - Encoding

- Demo time

  - Encode: https://elmah.io/tools/base64-image-encoder/

  - Decode: https://base64.guru/converter/decode/image

Part 2 - Encoding

- This can allow you to use things that you already have to represent **numeric values**

  - E.g., you might have (human) readable text (e.g., sending messages via SMS or emails)

    - Then you can use that to represent binary files (e.g., images)

      - Not all files are "texts", try to open an image file with notepad, it's unintelligible

      - But we can treat the binary file as a (big) number, then choose a "base" represent it with "digits" in text

Part 2 - Encoding

Following the same line of thinking, we can also get creative and use "**atypical**" character sets, e.g.,

- Base 2 (1 bit):
  '+' '-'

- Base 10:
  'A' 'B' 'C' 'D' 'E' 'F' 'G' 'H' 'I' 'J'

- Base 16 (4 bits):
  'A' 'B' 'C' 'D' 'E' 'F' 'G' 'H' 'I' 'J' 'K' 'L' 'M' 'N' 'O' 'P'