M2 CySec 23-24

« Advanced Security »

optionnal course

Misc. information

- **Schedule**
  - 2 x 3 hours a week (Wednesday afternoons and Thursday morning)
  - from November the 8th to December the 8th

- **Grading**
  - 3 ECTS
  - ~~labs~~ + project + oral presentation (coef. 0.5)
  - written exam (2hours, coef. 0.5)

- **Teaching staff**
  - L. Mounier + people from CEA + other teachers

Objective

Extends parts of the content provided by *regular courses*,
… with a focus on **software security**

Topics:

- reverse engineering
- (advanced) vulnerability detection, exploitation and analysis techniques
- HW/SW interface vulnerabilities
- Java security (access control, code integrity)
- code (de-)obfuscation techniques
- More on blockchains
- etc.

Course organisation

- a few **non formal** lectures
- **numerous** labs …
- one technical project (« ***in-depth analysis of a recent vulnerability*** »)
- an oral presentation of a **research paper**

brand new course material!

Project : study of a CVE

- **Objective**
  - Understand – and explain – a (recent) published **exploitable** CVE
  - (Try to) reproduce a **PoC** of the exploit
  - Discuss the existing/appropriate **patch /mitigation** options

- **Expected output (by group of 2)**
  - A **written report** (from 5 to 10 pages)
  - A short **presentation + demo** (~ 20 minutes)

- **Schedule**
  - From now to **December the 6th**

Main issue: choose a CVE

- **Related to a security topic you are interested in:**
  - Application level (including web vulnerability)
  - OS level (Windows, Android, etc. are welcome!)
  - Network component, firmware, HW/SW interface, Etc.

- **Well enough documented/understandable**
  - Poc exploit and patch information available

- **« Easy » enough to reproduce …**
  - Vulnerable code still available !
  - VM or Docker image of the exploit available?

How to proceed ?

- **Take the time to look for existing sources …**

  NIST CVE database: https://nvd.nist.gov/vuln/search

  Exploit database: https://www.exploit-db.com/

  Some known exploitable vulns: https://www.cisa.gov/known-exploited-vulnerabilities-catalog

  Google Zero RCA project: https://googleprojectzero.github.io/0days-in-the-wild/rca.html

  Numerous available blogs (security companies, independent (ethical) hackers, etc.)

- **Set up the appropriate environment you need …**
  - Docker (+ Dockerfile or docker image)
  - VM
  - Emulator?

- **Ask for help if necesary!**

Research paper presentation

- **Objective**
  - Understand – and explain – a (recent) research result
  - Choosen among a provided list of paper (or approved by the teaching staff)
  - Numerous security-related topics available …
- **Expected output (by group of 2)**
  - An **oral presentation** (~ 20 minutes)
- **Schedule**
  - From **November the 20th** to **December the 20th**
- **Remark**
  - Re-using available materials (slides, video, etc.) is allowed but:
    - Should be correctly credited …
    - Video replay is forbidden!