M2 CySec 26-27

« Advanced Security »

elective course

Objective

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

Topics:

- Reverse engineering and code (de-)obfuscation techniques
- HW/SW interface vulnerabilities
- Fault-injection attacks and counter-measures
- more on smart contracts
- IA and security … ?

IA and Security



brand new
course material!

- **IA for (software) security**
  - ML techniques for vulnerability detection/classification
  - LLM agents for software security analysis
  - (source code, binary code, reverse, use of code analysis, tools, etc.)

- **Security of IA-based systems**
  - Main threats/attack vectors
  - Existing counter-measures

Course organisation

- a few **non formal** lectures
- **numerous** labs … (about 75 % of the course volume)
- A few **external lecturers**
- An **oral presentation**:
  - either on a technical project (« ***in-depth analysis of a recent vulnerability*** »)
  - or on a research topic (**research paper presentation**)

Tentative Schedule (coarse grain)

Week 1: reverse-engineering

Week 2: code (de-)obfuscation

Week 3: Fault injection / Smart contracts

Week 4: Fault injection / Smart contracts

Week 5: Fault Injection

Week 6 and 7: IA and security

Week 8 : oral presentations

Misc. information

- **Schedule**
  - 2 x 3 hours a week
  - from November to the end of the semester

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

- **Teaching staff**

  L. Mounier + 3 CEA researchers + 1 UGA researcher

Oral Presentation

- **Subjects**
  - Either a **CVE study**
  - Or a presentation of a **research paper**
  - Work to be done **by groups of 2**

- **Schedule**
  - From **today** to beginning of January
  - Step 1 : choose between the 2 proposed subjects (**before Nov. 21st**)
  - Step 2 : choose a CVE or a research paper (**before Nov. 28th at last !**)
  - Step 3 : presentations during the **1st week of January …**

Beware, an oral presentation is also expected for the Phys. Security course !

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 5th**

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)
  - A short summary of the paper (~ 1 or 2 pages)

Remark

Resources available on the course web page

Re-using existing materials (slides, video, etc.) is allowed but:

- Should be correctly credited …
- Video replay is forbidden :-)

How to proceed ?

- **Choose a topic you are interested in:**
  - Software vulnerability analysis and detection
  - Web security
  - Attack countermeasures
  - Use of ML techniques for security
  - Reverse engineering techniques and/or code (de)-obfuscation
  - Security for mobile platforms (Android, iOS, etc.)
  - Malware detection and analysis, etc.

- **Find a well-explained paper (and slide set)**
  - USENIX security conference papers are good candidates …

- **Ask for help if necessary!**