Reverse Engineering — Summer 2018

Seminar

Julian Kirsch

Lehrstuhl für Sicherheit in der Informatik / I20
Prof. Dr. Claudia Eckert
Technical University of Munich

29. January 2018

"Block" Seminar

When? Wednesday, 12:00 - 14:00
01.08.033
Talks at the end of the semester

Where?

"Block" Seminar

When? **Wednesday**, 12:00 - 14:00
01.08.033
Talks at the **end** of the semester

Where? Seminartagungsstätte Frauenchiemsee
Disclaimer: Only if participants show interest!
Fallback: Room 01.08.033

Registration

- Registration using the **matching system**
- Solve a **reverse engineering challenge** instead (details on the course website).
- **Warning**: This semester we are dealing with real malware
- Submit a report about the analysis process and (optionally) a project proposal
- Submit your solution via e-mail no later than **2018-02-14, 00:00**.
- PGP-Fingerprint:

  `F949 CFBD 140A 6DD0 71E9 0B8C DC24 396B 6D45 1038`

- **8** slots (**FCFS** if I really have to, i.e. `solvecount` > 8)

Process

- Phase I: Find a **topic**
- Phase II: Find **literature**
- Phase III: Do your **reading / experiments / programming**
- Phase IV: **Writing** phase I
- Phase V: **Peer review**
- Phase VI: **Writing** phase II
- Phase VII: (Excursion &) Final **talks**

Process

- Phase I: Find a **topic**
- Phase II: Find **literature**
- Phase III: Do your **reading / experiments / programming**
- Phase IV: **Writing** phase I
- Phase V: **Peer review**
- Phase VI: **Writing** phase II
- Phase VII: (Excursion &) Final **talks**
- Phase IIX: **New:** Submission to ROOTS 2018

Exact schedule will be published once list of participants is known.
(Excursion is supposed to happen around end of the lecture period.)

Contents

- **Malcode** analysis
  - (de-)obfuscation
  - (un-)packing of binaries
  - ...
- **Static** analysis techniques
  - disassemblers
  - decompilers
  - symbolic execution
  - ...
- **Dynamic** analysis techniques
  - (anti-)debugging
  - symbolic execution
  - instrumentation
  - ...
- ...your (scientific) suggestion here

Questions?

F949 CFBD 140A 6DD0 71E9 0B8C DC24 396B 6D45 1038

Qualification task download provided via the course webpage.