

Reverse Engineering — SS 2019

Seminar

Clemens Jonischkeit, Fabian Franzen, Julian Kirsch

Lehrstuhl für Sicherheit in der Informatik / I20

Prof. Dr. Claudia Eckert

Technische Universität München

29th January 2019

"Block" Seminar

When? **Thursday** (bi-weekly), 13:00 - 14:30
01.08.033
Talks at the **end** of the semester



"Block" Seminar

When? **Thursday** (bi-weekly), 13:00 - 14:30
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**
- ▶ **No** letter of motivation
- ▶ Solve a **reverse engineering challenge** instead (details on the course website). Submit your solution via e-mail no later than **13th February 2019, 23:59**.
- ▶ PGP:
A903 76D1 65F3 25F9 8594 280A 2BA0 1592 EFAC B551
3FDE 8396 8B30 2707 0DE7 6CFF 3749 CEC2 ACC6 E196
- ▶ **8** slots (**FCFS** if we 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**: **Optional**: Submission to ROOTS 2019

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?

A903 76D1 65F3 25F9 8594 280A 2BA0 1592 EFAC B551
3FDE 8396 8B30 2707 0DE7 6CFF 3749 CEC2 ACC6 E196

Qualification task download (online today, 16:30):

[https://www.sec.in.tum.de/i20/teaching/ss2019/
reverse-engineering](https://www.sec.in.tum.de/i20/teaching/ss2019/reverse-engineering)