Reverse Engineering — SS 2020

Seminar

Fabian Franzen, Ludwig Peuckert

Lehrstuhl für Sicherheit in der Informatik / I20
Prof. Dr. Claudia Eckert
Technische Universität München

28th January 2020

What is reverse engineering?

> *Reverse engineering is the process of extracting the knowledge or design blueprints from anything man-made.*

Reversing: Secrets of Reverse Engineering
Eldad Eilam

- In this course: Targeting (probably **obfuscated**) software

Process

- Phase **I**: Select 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**: Final **talks**

Exact schedule will be published once list of participants is known.

Phase I

1. We will provide you with a list of our topics of interest
2. You will choose your own topic and:
    - Build a little tool (which the reverse enginieering world has always needed)
    - Reproduce the results of an exisiting conference paper
    - Create your own Systematization of Knowledge (SoK) paper
3. In all cases, you will put your work into context of exisiting literature
    - e.g at Usenix Security Symposium, S&P, ACM CCS, NDSS

Our Topics of Interest

- Advances in **Symbolic Execution**
- (Debugging) **Anti-Debugging Techniques**
- Obfuscation / Deobfuscation
- Virtual Machine Introspection (VMI)
- Techniques for **Decompiling** (Signature Generation / Reconstruction of Data Structures)

Process

- Phase **I**: Select 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**: Final **talks**

Exact schedule will be published once list of participants is known.

Registration

- Registration using the **matching system**
- **No** letter of motivation
- Solve a bunch of **reverse engineering challenges** instead (details on the course website). Submit your solution via e-mail no later than **12 February 2020, 23:59**.
- The flag format is `re20{...}` this year.
- Mail to:

  `re20-quals@sec.in.tum.de`
- **8** slots (**FCFS** if I really have to, i.e. `solvecount` > 8)

Time and Place

When?	Monday (bi-weekly), 14:00 - 16:00
	01.08.033
	Talks at the end of the semester
Where?	

Time and Place

When?	Monday (bi-weekly), 14:00 - 16:00
	01.08.033
	Talks at the **end** of the semester
Where?	Seminartagungsstätte Frauenchiemsee
	Disclaimer: Only if participants show interest!
	Fallback: Room 01.08.033

Grading

	40 %	Final Paper (Content, Style, Language, Scope, . . .)
	15 %	Experiments / Work on your tool
	10 %	Review
	30 %	Presentation (Content, Style, Timeliness, each **10%**)
	5 %	Discussion
Σ	100 %	Total

Questions?

`re20-quals@sec.in.tum.de`

Qualification task download (online today, 4pm):

`https://www.sec.in.tum.de/i20/teaching/ss2020/reverse-engineering`