Security Flaws — WS 2019/2020

Seminar

Fabian Franzen

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

16th July 2019

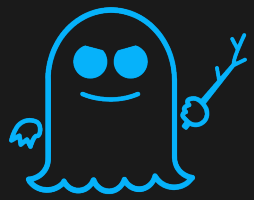
Overview

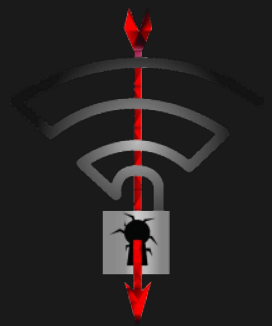
When? Monday (bi-weekly), 14:00 - 15:30
01.08.033
Talks at the end of the semester

Overview

When?	Monday (bi-weekly), 14:00 - 15:30
	01.08.033
	Talks at the **end** of the semester
Where?	Room 01.08.033

Contents





Process

- Phase **I**: Pick your favorite **security vulnerability**
- 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.

Deliverables

- Your **seminar paper** should contain
  - Description of the bug and the mechanism/protocol that contains the bug
  - Kind of Flaw (Buffer Overflow, SQL Injection, ...)
  - Impact on academic discourse
  - Description of the exploit
  - Techniques and experiments to discover/preventing it
- Your **final talk** should contain
  - Selected points of your paper
  - A small demo showing how to exploit the flaw
- Your **review** should contain
  - description of technical issues
  - suggestions how to improve writing
- Attendance at bi-weekly meetings is **mandatory**

Status meetings

We will have **bi-weekly** status meetings. In this meetings we will

- have **status presentations** by the students
- discuss how to write a paper, how to give a seminar talk
- discuss technical issues or **ideas**

Registration

- Registration using the **matching system**
- **No** letter of motivation
- Pwn a **challenge with a famous security flaw**:

  `nc honeynet.sec.in.tum.de 5556`

  Flag format: `sfs{...}`
- Submit your solution via e-mail to `franzen@sec.in.tum.de` no later than **24th July 2019, 23:59**.
- PGP:

  `3FDE 8396 8B30 2707 0DE7 6CFF 3749 CEC2 ACC6 E196`
- **8** slots (**FCFS** if we really have to, i.e. $\texttt{solvecount} > 8$)

Questions?

3FDE 8396 8B30 2707 0DE7 6CFF 3749 CEC2 ACC6 E196

This slides and more information:

https://www.sec.in.tum.de/i20/teaching/ws2019/security-flaws