Selected Topics of Secure Operating Systems

Bachelor/Master Seminar WiSe 2022/2023

Konrad Hohentanner and Vincent Ahlrichs

July 14, 2022

Fraunhofer

AISEC

Introduction & Motivation

Who are we?

- Department for Secure Operating Systems at Fraunhofer AISEC (Applied and Integrated Security)
- → Research and integration in industrial applications
- Department Topics
  - Confidential Computing
  - Kernel Security
  - Software Security
  - Embedded Security

AISEC Building at Lichtenbergstraße 11, Garching

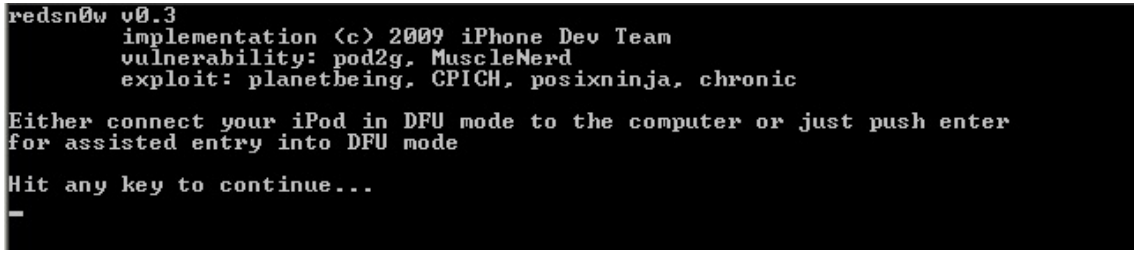
Our Goals for this seminar

- Get to know students interested in IT Security
- Learn from your great papers and presentations

Secure Operating Systems – Examples

Trusted Architectures

- Isolated and protected regions
- Verify integrity of running system/kernel from the beginning
- Secure Storage / Execution for high profile data (keys, boot measurements)

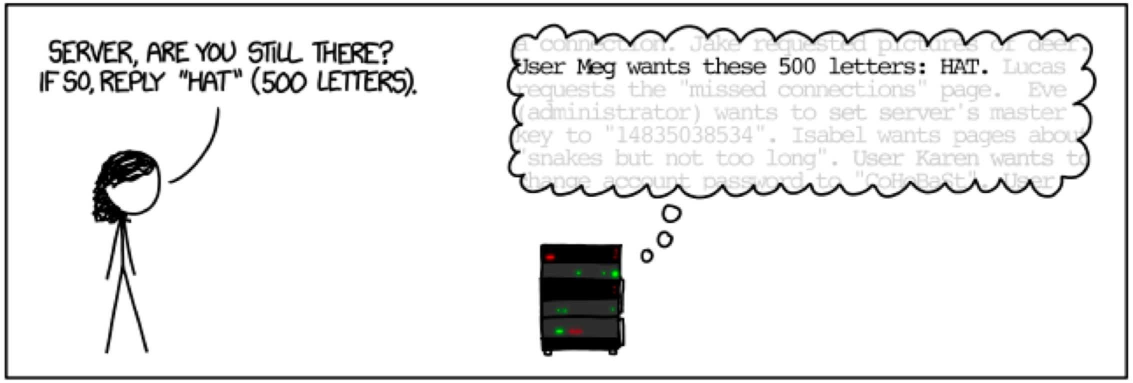


```
redsn0w v0.3
        implementation (c) 2009 iPhone Dev Team
        vulnerability: pod2g, MuscleNerd
        exploit: planetbeing, CPICH, posixninja, chronic

Either connect your iPod in DFU mode to the computer or just push enter
for assisted entry into DFU mode

Hit any key to continue...
_
```

Jailbreak, https://de.wikipedia.org/wiki/Jailbreak_(iOS)

Memory Safety and Fuzzing

- Find bugs
- Prevent bugs from creating vulnerabilities
- Allow integrated permission checks


SERVER, ARE YOU STILL THERE? IF SO, REPLY "HAT" (500 LETTERS).
a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User

Heartbleed, https://xkcd.com/1354/

Topic Suggestions

- TPM Bus Sniffing and Protections
- AMD SKINIT Secure Launch
- Intel Embedded Security (Programmable Services Engine)
- Intel TDX and its Remote Attestation
- ARM CCA and its Remote Attestation
- AMD SEV(-SNP) and its Remote Attestation
- Kubernetes Security
- Evaluation of Fuzzing
- IoT Fuzzing
- Fuzzing Seed Selection
- Hardware-based Memory Safety
- Redox OS
- Fuchsia OS
- Sculpt OS

- Students are welcome to suggest own topics
- Get some information about the topics and see if they interest you! (Good starting points are conference presentations on youtube etc.)

Prerequisites

- IN0009 Grundlagen: Betriebssysteme und Systemsoftware
- IN0004 Einführung in die Rechnerarchitektur
- preferable: IN2209 IT Sicherheit

Objectives

- Understanding of Secure Systems and attack vectors
- Preparing and writing a scientific paper in LaTeX (English, 9-10 pages IEEE)
- Presenting a scientific topic (german/english) 25-30 minutes + 15 minutes discussion
- Active participation

Grading

- Scientific Report: 50% (Content, Style, Effort, Grasp)
- Presentation: 30% (Content, Lecture Style, Understandability)
- Discussion: 10% (Participation)
- Peer Review: 10 % (2 Reviews à 1 page)

Registration

- Register in the TUM Matching system on time
- Short e-mail to vincent.ahlrichs@aisec.fraunhofer.de and monika.huber@aisec.fraunhofer.de
  - (mandatory) Your top 3 choice of topics (see suggested topics or own suggestion)
  - (optional) Why do you want to take this seminar?
  - (optional) Why do you chose a specific topic?
  - Deadline: **25.07.2022 23:59 CEST**
- Topic assignments based on choice & letter of motivation

Time Table

14.07.2022	Preliminary Meeting (today)
25.07.2022	Deadline for email with preferred topic choices
27.07.2022	Deadline for Registration TUM Matching
23.08.2022 13:00 h	Kickoff Meeting with Topic Distribution
24.10.2022	Deadline for Deregistration (afterwards 5.0 grade)
10.10.2022 23:59 h	Deadline Structure/Table of Contents
05.12.2022 23:59 h	Deadline Submission Review Paper
19.12.2023 23:59 h	Deadline Peer Reviews
11.01.2023 23:59 h	Camera-ready Version
16.01.2023 23:59 h	Slides
24.01. – 26.01.2023	Presentation meetings[1]

All deadlines are hard deadlines

[1] Presentation meetings will be held at Fraunhofer AISEC, if possible. Attendance required!

Contact Information

Vincent Ahlrichs, Monika Huber, Albert Stark

Department Secure Operating Systems

Fraunhofer Institute for Applied and Integrated Security

Address: Fraunhofer Institute AISEC
Lichtenbergstr. 11
85748 Garching b. München

Internet: https://www.aisec.fraunhofer.de/

E-Mail: vincent.ahlrichs@aisec.fraunhofer.de
monika.huber@aisec.fraunhofer.de
albert.stark@aisec.fraunhofer.de