Hardware Security Extensions

Bachelor/Master Seminar WiSe 2021/2022

Konrad Hohentanner and Vincent Ahlrichs

July 8, 2021

Fraunhofer AISEC

Introduction & Motivation

Who are we?

- Vincent Ahlrichs, Konrad Hohentanner
- Secure Operating Systems at Fraunhofer AISEC (Applied and Integrated Security)
- → Research and Integration in Industrial Applications
- Current focus on Fuzzing and Memory Safety

AISEC Building at Lichtenbergstraße 11, Garching

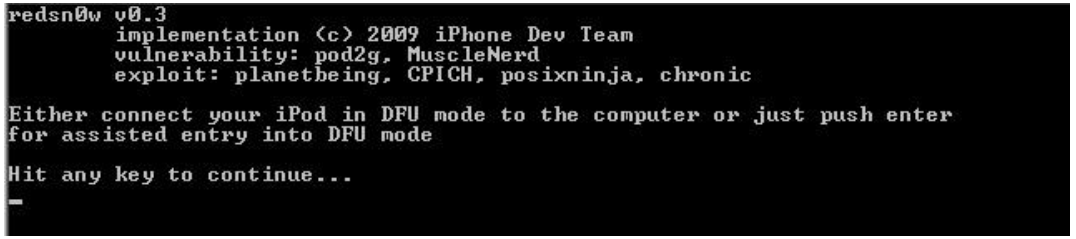
Our Goals for this Seminar

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

Hardware Security Extensions – Short Overview

Secure Hardware for CPUs

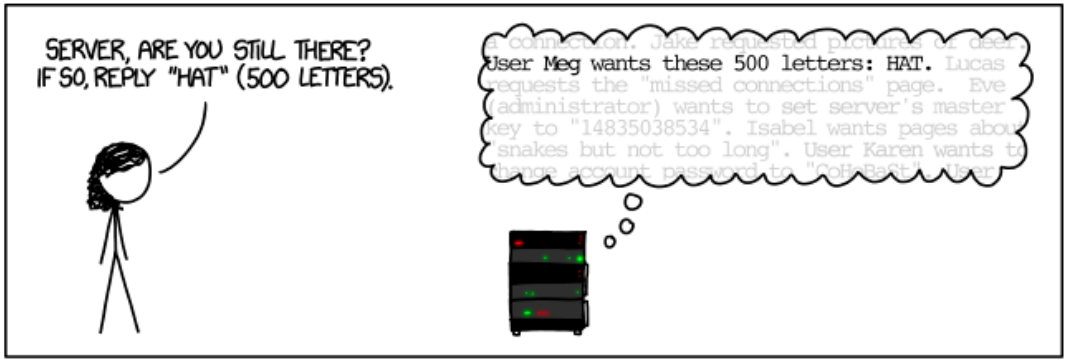
- Isolated and protected regions
- Verify integrity of running system/kernel from the beginning
- Secure Storage / Execution for high profile data (keys, boot measurements)



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

Memory Safe Runtime Environments

- Prevent bugs from creating vulnerabilities
- Allow integrated permission checks



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

Topic Suggestions

- CHERI architecture
- Memory Tagging
- Pointer Authentication Frameworks
- AMD SEV
- ARM TrustZone
- Intel Total Memory Encryption
- RISC-V Keystone
- History and Development of TPM
- ARM Security Hypervisor
- ARM v9 CCA

- 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, or

Prerequisites

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

Objectives

- Understanding of Hardware Security Extensions and attack vectors
- Preparing and writing a scientific paper in LaTeX (english, 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 Matching system on time
- Letter of motivation:
  - Your top 4 choice of topics
  - Why do you want to take this seminar?
  - Why do you chose a specific topic?
- Topic assignments base on choice & letter of motivation

Time Table

08.07.2021	Preliminary Meeting (today)
20.07.2021	Deadline for Registration
02.09.2021	Kickoff Meeting with Topic Distribution
25.10.2021	Deadline for Deregistration (afterwards 5.0 grade)
07.11.2021 23:59 h	Deadline Structure/Table of Contents
10.11. – 24.11.2021	Feedback Meetings for Structure
20.12.2021 23:59 h	Deadline Submission Review Paper
09.01.2022 23:59 h	Deadline Peer Reviews
12.01.2022	Feedback Review
30.01.2022 23:59 h	Camera-ready Version
06.02.2022 23:59 h	Slides
14.02. – 18.02.2022 (tentative)	Presentation meetings[1]

All deadlines are hard deadlines

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

Contact Information

Konrad Hohentanner and Vincent Ahlrichs

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/
Telefon:	+49 89 3229986-107 (Konrad) +49 89 3229986-114 (Vincent)
E-Mail:	konrad.hohentanner@aisec.fraunhofer.de vincent.ahlrichs@aisec.fraunhofer.de