Chair of Computer Engineering
Prof. Dr. Stefan Katzenbeisser
Florian Frank
Felix Klement

Passau, 14.12.2021

Winter Semester 2021/22

Hardware-Based Security

Exercise 4

Submission: 21.12.2021, 12:00, Übungskasten 1 (Exercise box 1) or StudIP
Discussion: 21.12.2021, 16:00-18:00 or 22.12.2021, 10:00-12:00

If you have questions about the exercises and their evaluation, please contact Mr. Florian Frank at Frank.Florian@uni-passau.de or Mr. Felix Klement at Felix.Klement@uni-passau.de.

In this Exercise, you can gather at most **35 points**.

1. Task: An Introduction to Hardware Trojans (25 points)

1. Give a definition for "hardware Trojans" and explain their properties in your own words. (3 points)
2. State two potential application areas that hardware Trojans can attack and briefly discuss them through an example for each. (4 points)
3. Give two examples of hardware Trojans from the news and explain what the issues were. (2 points)
4. Describe three different effects of Hardware Trojans. (3 points)
5. Hardware Trojans can be activated in different ways. Describe three different types of activations and describe a sample of each (3 points)
6. Describe how time bombs work. Also describe a scenario where a time bomb can be used? (2 points)
7. Describe how Dopant Trojans work? What is their effect? (4 points)
8. Explain in detail how two different categories of hardware Trojans work, i.e. how they are triggered and what their effects may be. (4 points)

2. Task: Prevention and Detection of Hardware Trojans (4 points)

1. In which types/categories can countermeasures against hardware Trojans be classified, according to the purpose they fulfill? What is the purpose and characteristics of each type? (4 points)

3. **Task:** Introduction to Side-Channel Attacks (6 points)

1. Explain the key idea behind timing side-channel attacks. (1 point)
2. Explain how power side-channel attacks work. (1 point)
3. Which countermeasures against side-channel attacks do you know about? What are their disadvantages? (4 points)