Hardware Security (NWI-IMC065)

Assignment 2: Reverse Engineering

IMPORTANT: This is a group assignment.

Grading: This assignment has nine (9) points obtained by answering all the questions correctly. You must obtain at least six (6) points to pass this assignment. Please check the questions for a breakdown of how the points are awarded.

Assignment	**Points**
Q1	2 points
Q2	2 points
Q3	1 point
Q4	2 points
Q5	2 point

Deadline: Tuesday, December 10, 2024, 23:59 sharp!

Handing in your answers:

- You can hand in your solutions via the assignment module in Brightspace.
- Make sure that your names and student numbers for both team members written on the envelope are on top of the first page!
- For submitting the answers, please submit a `.pdf` typeset solutions.

Your teacher will grade your assignment digitally in Brightspace.

1 Binary Reversing

Select firmware files by taking your group number modulo 4.
For example Group 7 will use `question1_3.elf` and `question2_3.elf`.

Question 1 *The device under test requires a password to be unlocked. Extract the correct password from* `question1_x.elf`. Answer the following questions:

- Find the adress of the function checking the password.
- Describe the method used to check the password.
- Give the password.

Question 2 *You have been given an old device that requires a licence key to be activate. Try to figure out the licence check using the leaked firmware:* `question2_x.elf`.
Answer the following questions:

- Find the adress of the function validating the licence key.
- Describe the method used to validate the licence key.
- Give two valid licence keys.

2 Firmware Reversing

Question 3. *Your friend is experimenting with hardware security and successfully extracts the firmware image of an old router. Your friend asks for help to reverse engineer the* `firmware.bin` *file.* Answer the following questions:

- What file signatures are present in `firmware.bin`?
- Can you identify the memory location where the different objects in the firmware are loaded from?
- Can you identify the bootloader name and version?
- How large is the kernel image?
- Analyze the entropy of the file and interpret the plot.
- Can you extract the file system of this firmware image?
- Is there anything else you can tell your friend about this file?

Question 4. *With your newly acquired skills for analyzing firmware, you decide to check the state of affairs by checking the firmware of an IoT device (router, webcam, etc.) manufacturer's website.*
Find a firmware image that piques your interest and download it. Analyze this file and describe all you can find about the downloaded firmware (you can use question three as guidance to format your answer). Include the download link.

Question 5. As most firmware for IoT devices was not developed with security in mind, tools such as and Firmwalker have been proposed to automate the security analysis. Please describe what the tool does, use it on the extracted file system from `firmware.bin`, and formulate an opinion on its usefulness.