more security. usd

Hacker Contest

WS17/18 Registration Challenge

usd AG

Author Almon, Ralf
Date 01.10.2017

1 Introduction

The Hacker Contest is a course which requires quite some time and the ability to independently explore new topics. Therefore, the selection of students will be done with this registration exercise. Please be aware that you do not have to complete the exercise fully to register to the course. If you complete more challenges, your chances will increase to be accepted. If there are only few registrations, even a small number of answered question can get you a seat.

Please be aware, that the registration challenge is divided into three difficulties. If you have only a small amount of time, you should do the easy task. If you have more time you could try the medium one. If you are ready for a challenge do the hard one. If you do the medium or hard challenge, please use the files you obtain to continue. The binaries differ, so that you get the full credit if you solve the hard or medium task completely. The result will always be scripts as the ones you can find in the easy zip. But they will differ in some aspects depending on the challenge you obtained them from.

1.1 Submission policy

You should answer all the questions that you can in a textual form. **In addition to the plain answer, you must provide how you got the answer.** For example, if you are able to analyze the update csv file you should give a brief summary of the following: Which tools have you used, for which purpose, etc.
The submission is done by mail. You must **not** work in groups.
Please provide your answers in **one** file. You must use the **PDF** file format. You must provide the following information on the first page of your document: name, matriculation number and your own mail address.

The submission deadline is the 13. October at 23:59:59. The timestamp of the receiving mail server determines the time of your submission. So you should send it in time.

Please send your submission to hackercontest-hda@usdmailer.de

If you have any questions about the tasks, feel free to contact us at hackercontest-hda@usdmailer.de. For fairness, we cannot provide you with any help how to solve the task. If you want to solve the medium or the hard task: try harder.

2 Task

2.1 Setting

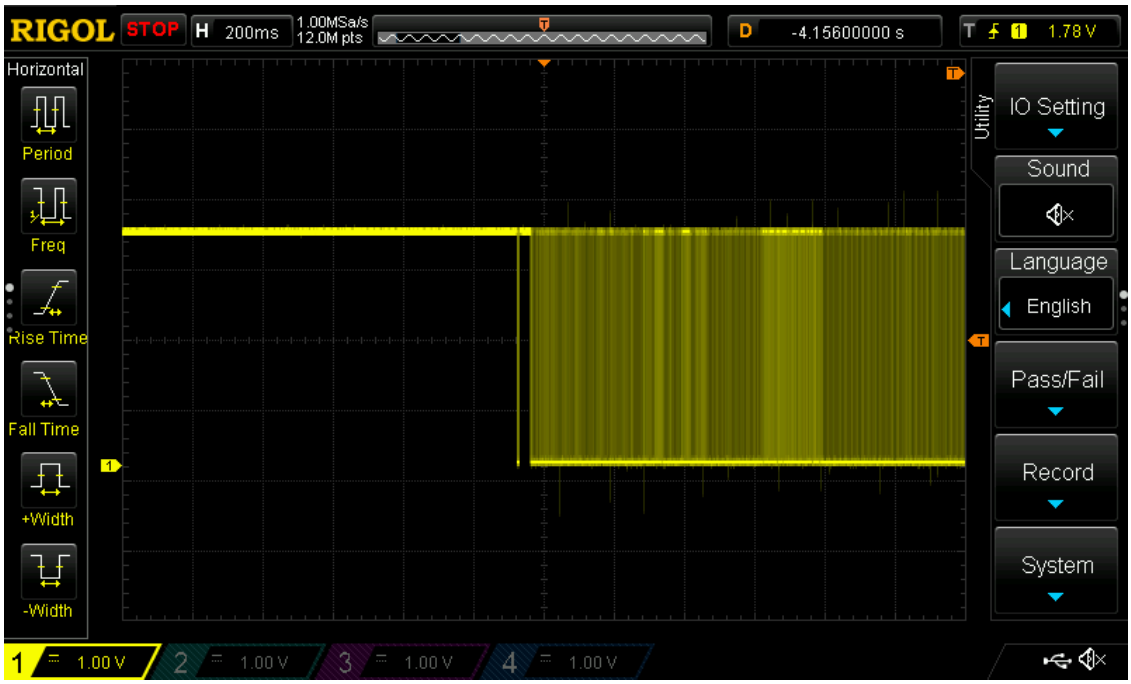
Your company has the task to make a security review of an update process of a simple electronic locking system. The system is built into the wall. The only visible parts are a green and a red LED as well as a 4x4 keypad with the digits from 0-9 and some additional buttons A,B,C,D,# and *. It also features a hidden port with two PINs. This port is used for conducting software updates and adding new features to the lock.
A colleague of yours already examined the update process and did some tests on it. In the last test, he sadly destroyed the lock and quit his job.
Your task is it now to use the data he already acquired to answer a couple of questions.

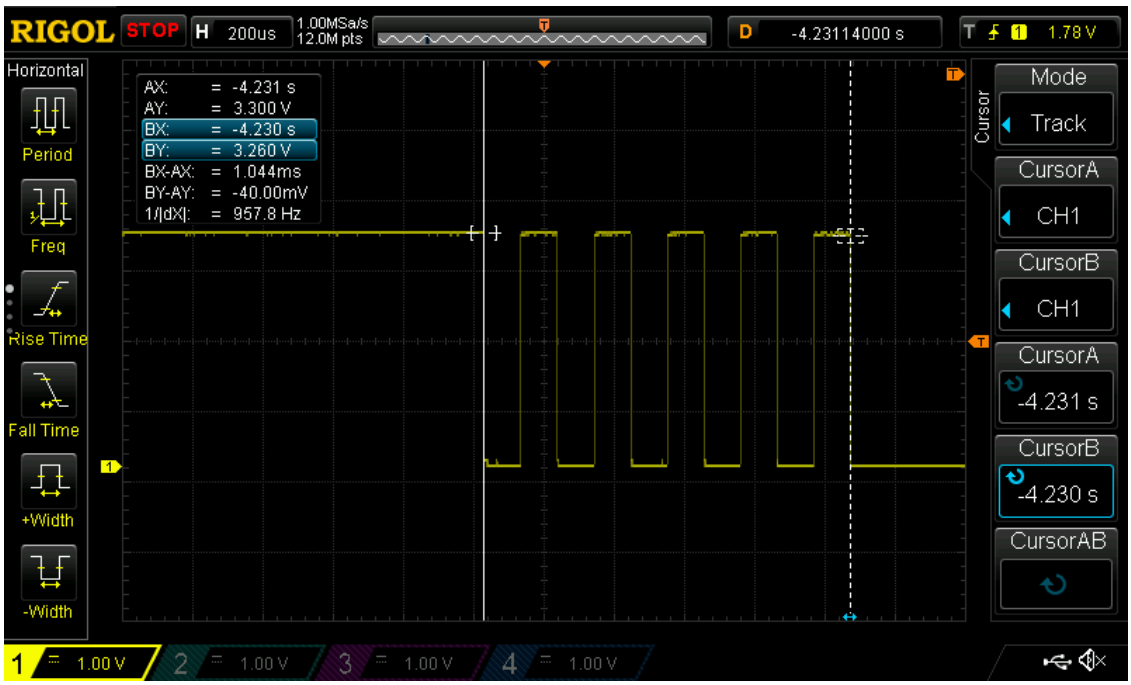
2.2 Difficulties

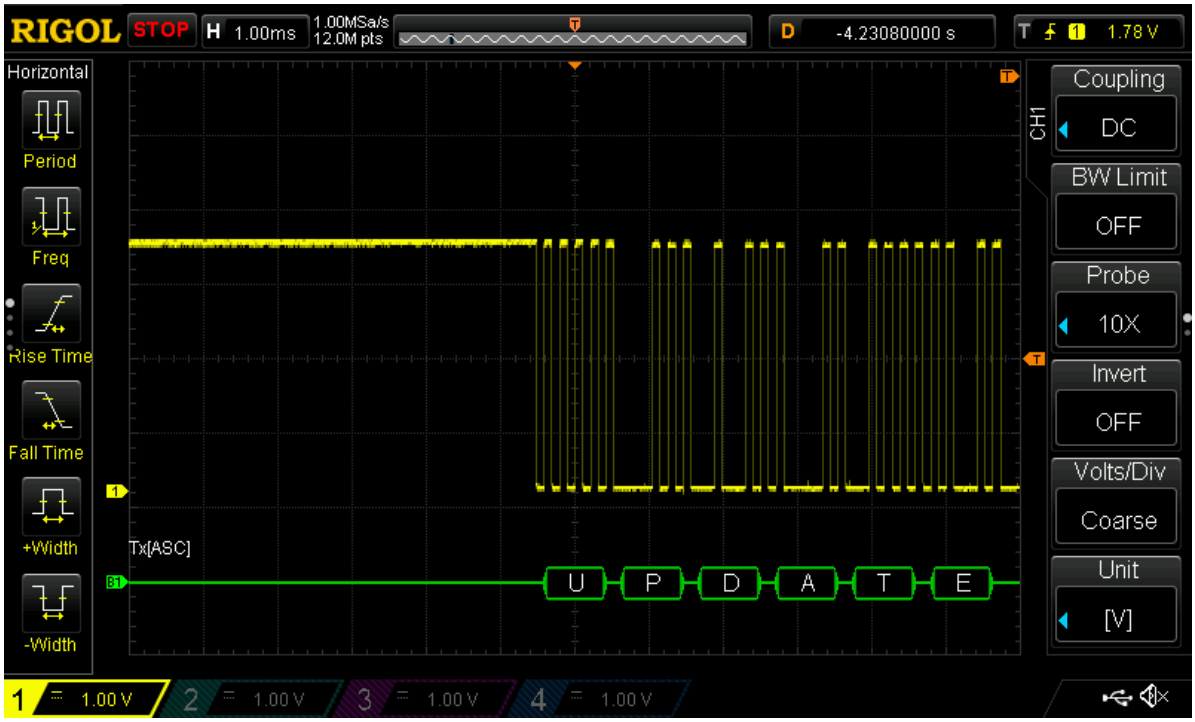
In the following, you can see the different difficulties. Depending on where you start, your colleague had time to work further, so that you can focus on later steps of analysis or he quit earlier, and you have to do more. Please note that the content of the different difficulties differ. This way you can prove that you got a file from a certain difficulty instead of just pulling it from an easier step.

2.2.1 Hard

Your colleague used a multi meter to check the voltage on the lines. He discovered, that one line to the other had a potential of 3.3V. He hooked up the update module to the port, connected his oscilloscope in parallel, and took some pictures. Apart from these screenshots, he only saved a strange file which is inside the hard challenges zip file.







2.2.2 Medium

Your colleague extracted some kind of binary file from the update process. You can find it inside the medium zip file.

2.2.3 Easy

Your colleague had the time to extract some interesting python scripts from the binary file he got from the intercepted update process. He included them in the easy zip file.

2.3 Task

In the following are some questions you need to answer. For every step there are separate questions. Please use the “hardest” difficulty file that you have for answering the questions.

2.3.1 Update Transmission (hard mode)

- What kind of communication is used for transmitting the update?
- What is the transmission rate used?
- Which sample rate was used to capture the data?
- Can you describe in easy words which data gets transmitted?
- Which hash gets transmitted? What kind of hash is it?
- What is the sha1sum of the transmitted file? Please note that file command should return a ELF binary format on the file you obtained. Also double check that you don’t have a new line as last byte of the file.

2.3.2 Update Binary (medium mode)

- What architecture is the binary?
- Can you obtain any information about the used platform from the binary?
- Which command line argument is necessary for a successful update?
- How does the binary work? Which commands does it invoke?

2.3.3 Keypad Scripts (easy mode)

- What is the factory default PIN (PLEASE use the “hardest”-mode script you acquired to answer this question)
- Can you spot a flaw in the implementation of the keypad?
    - Do you think the flaw was a mistake or intended?
    - Which keypresses are necessary to exploit the flaw?
    - Please give the complete console output of the script for a successful exploitation.