Title of the Experiment: Hardware Trojan Attacks II

Group Members' Names: Sujan Kumar Saha, Pankaj Bhowmik

Date: 10/01/2019

Abstract

This experiment is about hardware trojan attack. The hardware trojans are activated at certain condition which is named as trojan trigger condition. In this experiment, we used a physical parameter "temperature of the chip" to activate a trojan in the circuit. In the first part of the experiment, we design our system using internal ADC of the MAX 10 FPGA, PLL and RAM. We use that design to measure the on chip temperature value of the FPGA and show it in memory content window. In part two, we showed that value in the LEDs and 7-segment display. In part 3, we implemented a temperature triggered trojan. In the optional part, we implemented the sequential trojan where it is activated after exceeding the temperature value two times sequentially. We observed the effect of changed data in the memory.

Experiment Details

Goals: The goal of this experiment is to understand the working principle of a hardware trojan and its activation mechanism

Experimental Setup: We used the MAX10 FPGA on Hardware Hacking (HaHa) board, USB-blaster and Quartus Prime Software on a computer for this experiment.

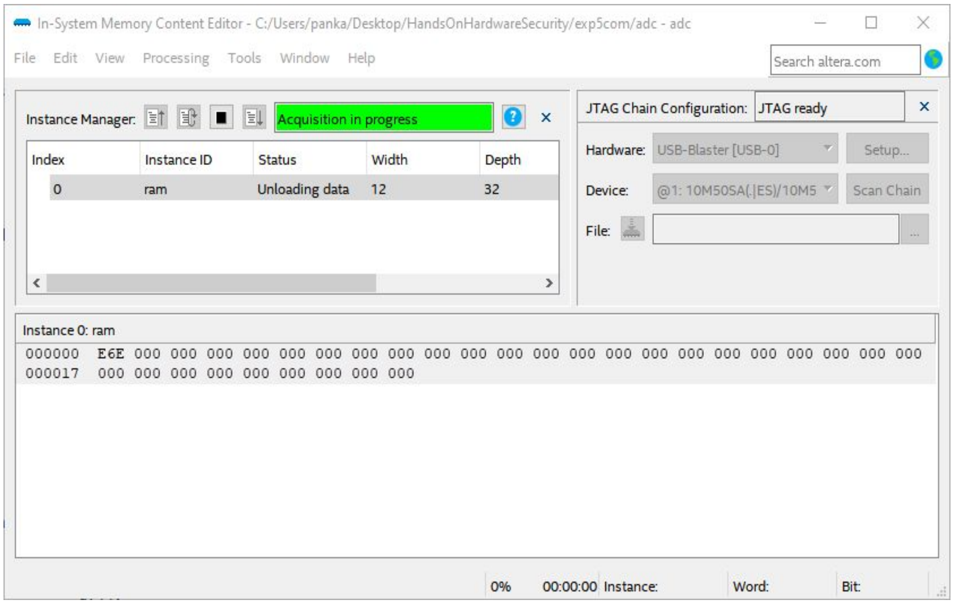
Experiment Steps:

1. We designed our target system using built-in ADC, PLL and RAM IP core in Quartus with proper configuration and connection.
2. We loaded the bitstream to the FPGA and checked the corresponding results in in-system memory content editor window.

Results and Analysis:

Part I:

1. The code is attached to the report. (part1.v)
2. The output value of the temperature sensor was **E6E** which represents 19 degree celsius. This measurement is showing room temperature. Hence the reading is pretty close to the ideal case. The content of the RAM is shown in the following figure.


In-System Memory Content Editor - C:/Users/panka/Desktop/HandsOnHardwareSecurity/exp5com/adc - adc
File Edit View Processing Tools Window Help
Search altera.com
Instance Manager:
Acquisition in progress
JTAG Chain Configuration:
JTAG ready
Setup...
Scan Chain
File:

Index	Instance ID	Status	Width	Depth
0	ram	Unloading data	12	32

Hardware: USB-Blaster [USB-0]

Device: @1: 10M50SA(.|ES)/10M5

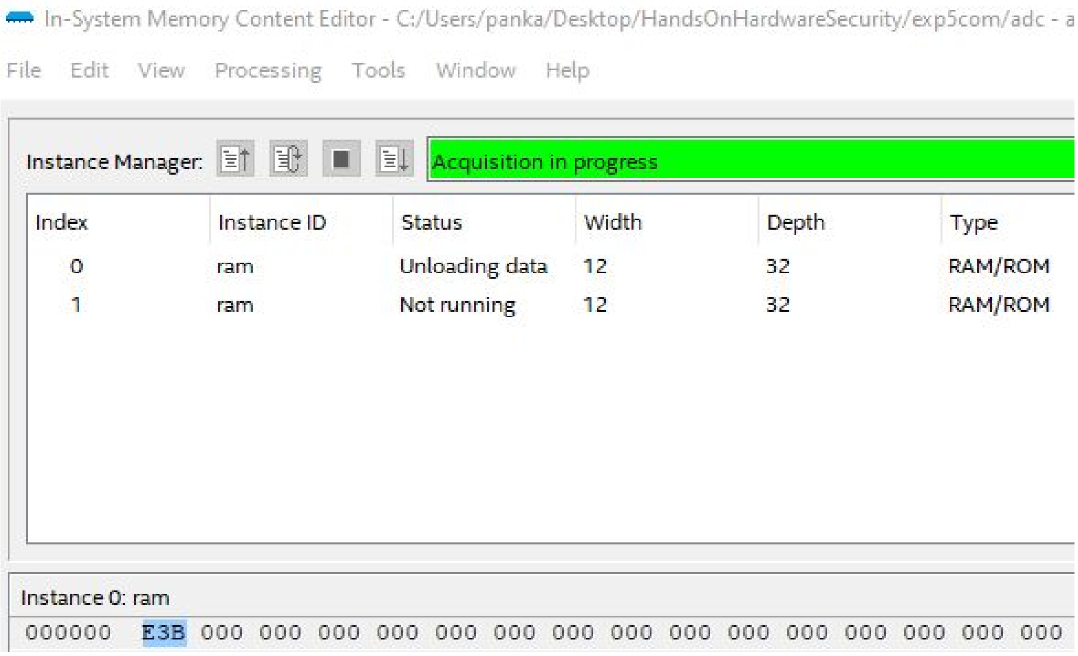
Instance 0: ram

```
000000  E6E 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000017  000 000 000 000 000 000 000 000 000
```

0% 00:00:00 Instance: Word: Bit:

Figure 1: Temperature code in the in-system memory content window

3. Under 40 degrees celsius, the output is E3B in the memory and the screenshot is attached.


In-System Memory Content Editor - C:/Users/panka/Desktop/HandsOnHardwareSecurity/exp5com/adc - a
File Edit View Processing Tools Window Help
Instance Manager:
Acquisition in progress

Index	Instance ID	Status	Width	Depth	Type
0	ram	Unloading data	12	32	RAM/ROM
1	ram	Not running	12	32	RAM/ROM

Instance 0: ram

```
000000  E3B 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
```

Figure 2: Temperature code at 40 degree celcius

Part II:

4. In our design, we showed the temperature value using 7-segment display and LEDs. We can see 12 bit temperature value from in-system memory content editor. We showed the most significant 4 bits to 7-segment display and used 8 LEDs to show rest 8 bits of temperature value. Below is a

screenshot of that which shows the temperature value E6A. We have attached the verilog code. (part2.v)

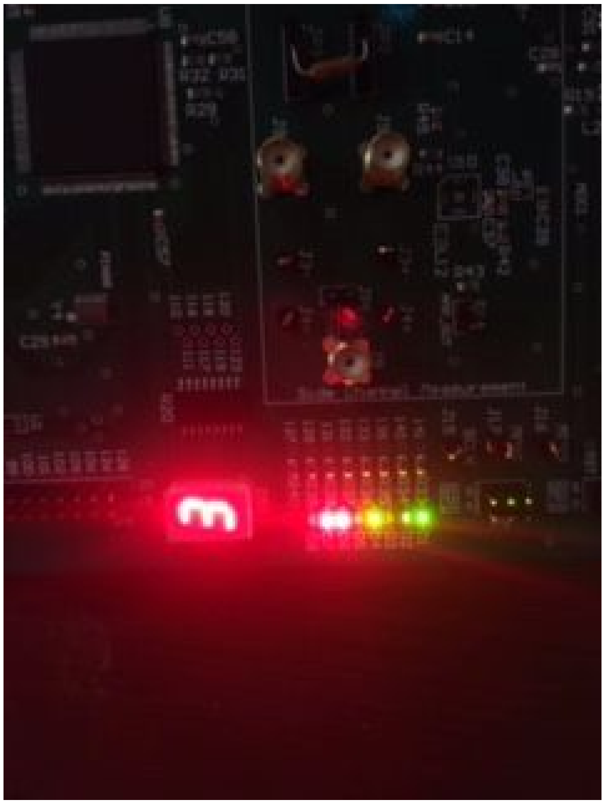


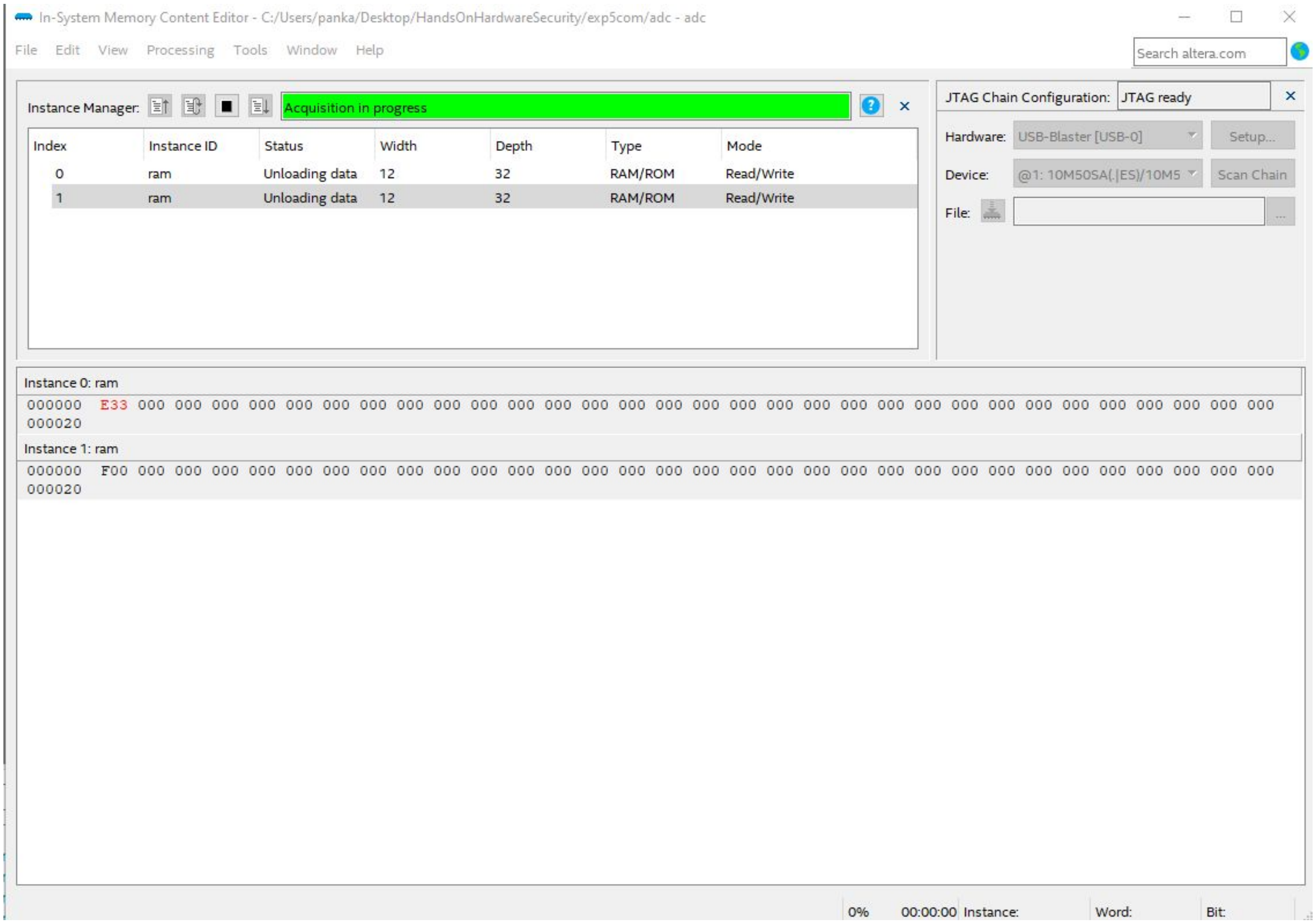
Figure 3: The temperature code showing in 7-segment display and LEDs

5. Our design receives temperature data from RAM output port q and process it to send to LEDs and 7-segment display. The screenshot is already given in figure 3.
6. Our design uses 440LEs in the FPGA.

Part III:

7. For part III, we used another instance of RAM and kept a data “0FF” in that memory when trojan is not triggered. When the trojan is triggered the data is inverted which is “F00”. The trojan is triggered when the temperature is 40 degree celcius.
8. The payload of the trojan is inverting the value of the second RAM. We observe the change of the value in the in-system memory window second RAM instance. The figure 4 shows the value while trojan is activated (Temperature is higher than 40 degree celcius) and figure 5 shows the value when trojan is not triggered (Temperature is less than 40 degree celcius).
9. After inserting the trojan, the LE usage is 552. So, the hardware overhead is (552-440)/440 = 0.2545 or 25.45%.
10. The verilog code of the top module is attached with the report. (part3.v)

11. Referring to figure 2 of the given document, our trojan is a combinational digital triggered trojan and digital memory content payload as the trojan is changing a value in the memory location.


In-System Memory Content Editor - C:/Users/panka/Desktop/HandsOnHardwareSecurity/exp5com/adc - adc
File
Edit
View
Processing
Tools
Window
Help
Search altera.com
Setup...
Scan Chain
...

Instance Manager: Acquisition in progress

Index	Instance ID	Status	Width	Depth	Type	Mode
0	ram	Unloading data	12	32	RAM/ROM	Read/Write
1	ram	Unloading data	12	32	RAM/ROM	Read/Write

JTAG Chain Configuration: JTAG ready

Hardware: USB-Blaster [USB-0]

Device: @1: 10M50SA(.|ES)/10M5

File:

Instance 0: ram

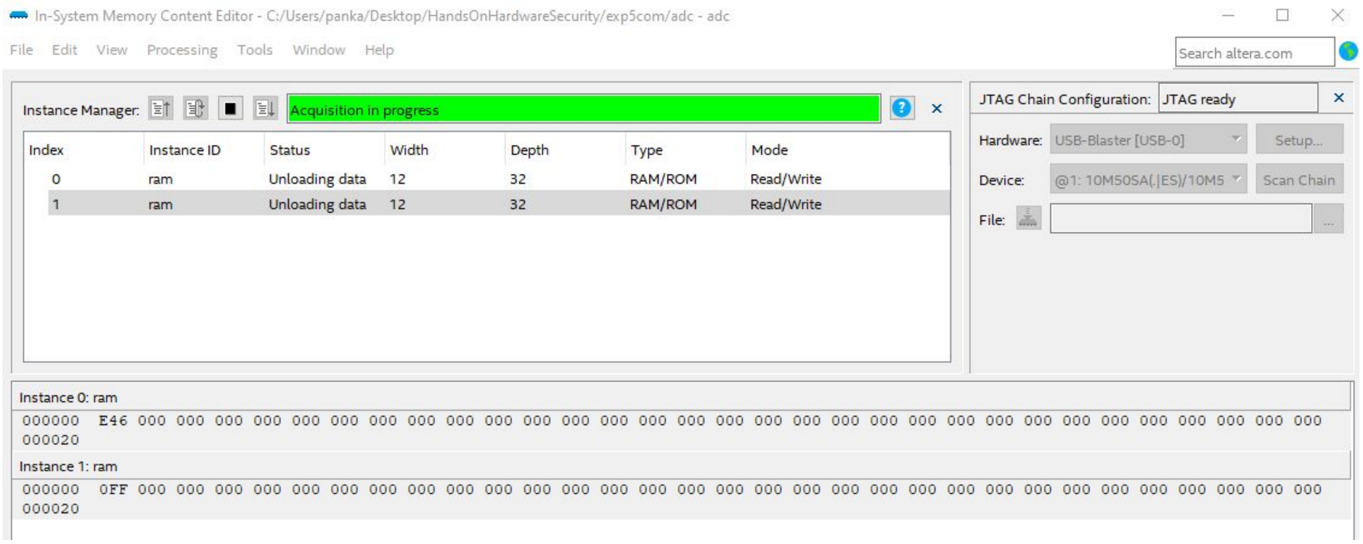
```
000000  E33 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000020
```

Instance 1: ram

```
000000  F00 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000020
```

0% 00:00:00 Instance: Word: Bit:

Figure 4: The memory value when the trojan is activated


In-System Memory Content Editor - C:/Users/panka/Desktop/HandsOnHardwareSecurity/exp5com/adc - adc
File
Edit
View
Processing
Tools
Window
Help
Search altera.com
Instance Manager:
Setup...
Scan Chain
File:
...

Acquisition in progress

JTAG Chain Configuration: JTAG ready

Hardware: USB-Blaster [USB-0]

Device: @1: 10M50SA(.|ES)/10M5

Index	Instance ID	Status	Width	Depth	Type	Mode
0	ram	Unloading data	12	32	RAM/ROM	Read/Write
1	ram	Unloading data	12	32	RAM/ROM	Read/Write

Instance 0: ram

```
000000  E46 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000020
```

Instance 1: ram

```
000000  0FF 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000
000020
```

Figure 5: The memory value when the trojan is not activated

Part IV:

1. We have implemented part IV of this experiment. It is a sequential trojan. We have attached video for that.
2. It’s hardware overhead is same as the sequential trojan implementation which is 25.45%.
3. We attached the verilog top module for this implementation. (part4.v)

Summary and discussion:

In this experiment, we have implemented a hardware trojan which is activated based on the change of a physical parameter value (Temperature). Our designed trojan changes a value in the memory which might be an important data for a system. In regular temperature the memory content is not corrupted but at high temperature (higher than 40 degree celcius), the memory content value is inverted. For the last part, we have implemented a sequential trojan where the trojan is activated after increasing the temperature of the chip two times sequentially .