COST STSM Final Report

ICT COST Action IC1204: TRUDEVICE

COST STSM Reference Number: COST-STSM-IC1204-17448

Barış Ege
Digital Security Group - ICIS
Radboud University Nijmegen

June 3, 2014

1 Mission Statement

The aim of the scientific mission was to investigate the effect of ambient temperature on the types of faults that can be generated through clock or power glitching. Previous works utilizing temperature changes covered either fault injection through only heating up the device [1], or cooling it down which led the attacker to recover the memory contents after the device was powered off for several seconds [2]. However changing the ambient temperature that the device is running in, changes the physical behaviour of the device and in turn can result in generation of faults with different glitch parameters than required in room temperature. We were further interested in the range of glitch parameters that can potentially be influenced by the ambient temperature, which in turn can lead to injecting reproducible faults with a wider range of parameters, and therefore increasing the success probability of a fault attack.

2 Experiments and Results

In our experiments, we used a custom made fault injection board, utilizing a Field Programmable Gate Array (FPGA). This board enabled us to inject reproducible clock glitches to our target, an ATmega162 microcontroller, with high accuracy. We first focused on profiling what kind of faults can be generated with the available setup we had, in room temperature. This resulted in the observation of 3 different kinds of faults:

- Inconsistent faults resulting in an unpredictable behaviour of the device,
- Faults that affect the instruction decoder,
- Faults that affect the program counter.

Interesting fact here is that it was never before documented that the program counter of an ATmega162 device could be affected through clock glitching. Moreover, the faults affecting the instruction decoder were predictable and reproducible when the same parameters were used for injecting a clock glitch.

We profiled these faults through running numerous experiments with different initial values for the internal registers of the microcontroller and verified that the results we got were independent of the values written in the registers initially. This lead us to the conclusion that the instruction decoder is in fact affected and not the arithmetic logic unit (ALU) of the device.

After profiling the device in room temperature, we repeated the experiments when the device is heated up to 100° C. For heating, we used a laboratory heating plate from Schott instruments (SLK 1), and for the temperature measurements we have used a PT100 sensor element. Since the heating plate had no digital input, we had to adjust the heat depending on the measured temperature on the sensor by hand and keep it at the target temperature range. This introduced a ±2° C error margin for the ambient temperature of the device but our results were reproducible for the given temperature.

Figure 1 presents different types of faults we were able to produce in relation to the ambient temperature and the glitch parameters that we have used for clock glitching. On the vertical axis of the figure the different types of faults are listed, and on the horizontal axis the delay we have used to introduce a clock glitch within the clock cycle where the target instruction (`ADD R16, R5`) was executed.

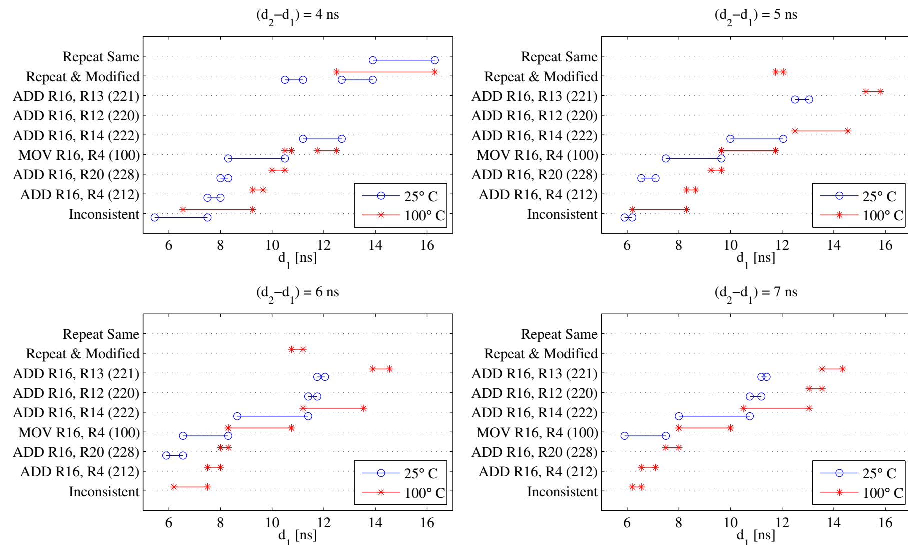

Figure 1: Types of glitches generated depending on the glitch parameters used and the ambient temperature, while executing the instruction `ADD R16, R5`. The device is clocked at 20 MHz for these experiments.

Results presented in Figure 1 in fact shows that with increased ambient temperature, the device gets more vulnerable to clock glitching and for a given glitch parameter, some faults can only be generated when the device is heated up.

3 Future Work

In this mission, we investigated the effect of ambient temperature on the types of faults that can be generated through clock glitching. However, during the entire set of experiments, we always stayed within the boundaries that are documented in the specification of the target microcontroller. As future work, we plan on working with a more precise heating element (e.g. a resistor-based one) to improve the precision of our test setup and heat up the target device to higher temperatures beyond the limits of the device to see if we can improve our results.

References

[1] Michael Hutter and Jörn-Marc Schmidt. The Temperature Side-Channel and Heating Fault Attacks. In *Smart Card Research and Advanced Applications - CARDIS 2013, 12th International Conference, Berlin, Germany, November 27-29, 2013, Proceedings.*, Lecture Notes in Computer Science, 2013. in press.

[2] Sergei Skorobogatov. Low temperature data remanence in static RAM. Technical report, University of Cambridge Computer Laboratory, June 2002.