# Defending electronic systems against hardware attack

Raúl Jiménez Naharro, Fernando Gómez Bravo, Juan Antonio Gómez Galán, Manuel Sánchez Raya and Juan José Mata de Acuña

Departamento. Ing. Electrónica, de Sistemas Informáticos y Automática
ETSI La Rábida, University of Huelva, Huelva, Spain
{naharro, fernando.gomez, jgalan, msraya, -}@diesia.uhu.es

***Abstract*—Hardware attack is becoming an important scenario in the system design. Pupils who study design of electronic and computer systems must know this scenario and possible solutions against this kind of attacks. This work is a set of exercises to know some vulnerabilities in electronic and computer systems depending on the behavior implementation. Two cases of studies will be considered: timing attack and differential fault analysis (DFA). The study of each attack will be divided into three stages: the use of the vulnerability as attack; the study of the vulnerability; and the elimination or reduction of it.**

***Index Terms*—Hardware attack and security, attacks based on analysis, education in computer science.**

## I. INTRODUCTION

This work is implemented in the course "Ataque y Seguridad Hardware", an optative course in Máster en Ingeniería Informática in Escuela Técnica Superior de Ingeniería La Rábida, University of Huelva. The main objective of this course is to show the vulnerabilities that can be exploited by hackers, and to reduce them to obtain a more secure system.

## II. DESCRIPTION OF WORK

The exercises will use a verification system of passwords in order to show its vulnerabilities. This system will verify a 32 bits password, using four packets of 8 bits. The input password will be compared with the valid passwords stored in a data base. This comparison will be used to obtain the access of the system. Therefore, a brute force analysis requires $2^{32}$ combinations to test. The verification system is compounded by three modules: an input data module (to introduce the packets of 8 bits), a memory module (to store the data base of passwords), and a controller module (to implement the verification algorithm). The controller will be implemented as a specific application system and as a system based on a microcontroller (concretely PicoBlaze™ [1]). Then, the vulnerabilities will be studied in a wired and a programmed system with the same functionality. Both systems will be used in order to analyze the implementations of hardware attacks. The objective of the attacker will be to achieve the access without the knowledge of a valid password and without using the combination of brute force analysis. In the case of timing attack, the attacker will only need to access to the input and output ports (always accessible in any system). In the case of differential fault analysis, the attacker will need to access to the signals that indicate the behavior of the system (state signals in the wired system, and program counter in the programmed system). Once, the sources of vulnerabilities have been identified, the pupils must modify the verification algorithm to eliminate or reduce them. The objective of the defense will be to avoid the objective of the attack, that is, knowing a valid password and/or needing a brute force analysis to obtain the access.

## III. RESULTS

The results obtained in this work will be the behavior of a system in non-attack and attack scenarios, and in an attack scenario with implemented countermeasures. Such exercises will be implemented in practice using VHDL. This code will be used to program a FPGA device (concretely, a low cost model, Spartan 3E100 [2]). The main interest of the education will be centered in the defense. So, the more problematic details of the implementation of attack modules will not be considered (such as the access to internal signals).

## REFERENCES

[1] http://www.xilinx.com/support/documentation/ip_documentation/ug129.pdf
[2] http://www.xilinx.com/support/documentation/data_sheets/ds312.pdf