Athens Institute for Education and Research
ATINER

ATINER's Conference Paper Series
COM2012-0162

Protection Piracy on Embedded System

José Ivo Fernandes de Oliveira
Professor
IFMT - Federal Institute Science and Technology of Mato Grosso
MT, Brazil

Athens Institute for Education and Research
8 Valaoritou Street, Kolonaki, 10671 Athens, Greece
Tel: + 30 210 3634210 Fax: + 30 210 3634209
Email: info@atiner.gr URL: www.atiner.gr
URL Conference Papers Series: www.atiner.gr/papers.htm

Printed in Athens, Greece by the Athens Institute for Education and Research.

ISSN **2241-2891**
12/09/2012

An Introduction to ATINER's Conference Paper Series

ATINER started to publish this conference papers series in 2012. It includes only the papers submitted for publication after they were presented at one of the conferences organized by our Institute every year. The papers published in the series have not been refereed and are published as they were submitted by the author. The series serves two purposes. First, we want to disseminate the information as fast as possible. Second, by doing so, the authors can receive comments useful to revise their papers before they are considered for publication in one of ATINER's books, following our standard procedures of a blind review.

Dr. Gregory T. Papanikos
President
Athens Institute for Education and Research

This paper should be cited as follows:

Fernandes de Oliveira, J.I. (2012) "**Protection Piracy on Embedded System**" Athens: ATINER'S Conference Paper Series, No: COM2012-0162.

Protection Piracy on Embedded System

José Ivo Fernandes de Oliveira
Professor
IFMT - Federal Institute Science and Technology of Mato Grosso
MT, Brazil

Abstract

In recent years, embedded systems present in electrical and electronic devices have become widespread refined and improved, and they offer greater convenience in human life. For these reasons, there have been a variety of researches in this line. The main feature of these systems, in contrast to general purpose systems, is its high interaction with electronic products in different situations that require real-time capabilities. In this context, the security of the embedded systems has become considerably important in that it forms also have sophisticated piracy. Among the various forms of attacks to the vulnerabilities of systems, stand out external attacks exploiting flaws left in the project by developers or by software companies do not consider security as a requirement due the lack of time or financial resources, or the belief that legal protection should be sufficient. This article aims to show the relevance of the use of development techniques and project management whose primary focus is the protection of embedded systems implemented in FPGA using Bitstream encryption code, thereby ensuring intellectual property and lifecycle of the application.

Keywords: Piracy, Embedded Systems, intellectual property, FPGA, Bitstream.

Contact Information of Corresponding author: jose.oliveira @ cnp.ifmt.edu.br

1. Introduction

The diversity of technologies in the global market today, not only opened doors to new career opportunities, they also appeared with the crimes of piracy. These crimes range from simple forgery to espionage and are faced by corporations, institutions and government agencies. The piracy explores the weaknesses in security systems design to copy and sell illegal products in the black market with a very low price. For example: DVD copies containing software, games or movies, system on chip, processors, dedicated hardware and large systems. These crimes can have far-reaching consequences that go far beyond the crimes against intellectual property or financial loss of a corporation or an institution. The objectives of those who commit such crimes can range from the simple pleasure of achieving success on purpose "*I win*", or the desire for fraudulent gains without making the slightest investment or to learn the capabilities of other systems and use the knowledge gained to start your own development of their projects (Reverse Engineering).

2. Global Scenario

Multinational companies that sell their products in countries where the institutions responsible (Government and Society) cannot suppress piracy suffer a loss of market and are forced to develop new strategies to create value and enhance market performance adversely. The piracy creates a ripple effect on the economy and, in loss to revenue for the software and hardware industry, low gains for service companies and distribution related to information technology. According to the Business Software Alliance - BSA, which conducted a study, published in 2010, involving 42 partner countries, spending on information technology has grown almost 60% faster than the rest of the economy, about 1.2 millions of businesses selling, distributing software, hardware and services. In the countries studied, these companies employ about 13 million people. Also according to this report estimated that the rate of software piracy for PCs (Personal Computer) in 2009 was 43%, meaning that more than four out of 10 applications are installed without a license and that the commercial value of software amounted more than US$ 51 billion. Another quite significant fact, the report pointed out, is that if the BSA's member countries reduce piracy by 10% over four years (2010 to 2013), the software industry would inject about US$ 142 billion dollars in the global economy would create approximately 500,000 new jobs and generate around US $ 32 billion tax to the government. BSA is the representation of industry software and hardware in the world with governments and the global market (BSA, 2010).

Response Actions

U.S. awareness of the crimes of piracy made the security community responded with a set of policies and standards that form the basis of safety systems. Among them, there is the DoD Directive 5200 - Defense of Department. It is a set of policies, standards and practices established to protect

and defend the defense information and information systems of government. One of the objectives of the strategy is to protect "reliable data and their platforms" This guidance also applies to a specific hardware. This policy, which drives the development of anti-counterfeiting features to DoD programs. This policy applies to all information systems, including the following systems: Autonomous, Communications networks of computers of all sizes, analog/ digital, or both technologies, their associated peripheral devices, Software process control, Embedded Systems, Firmware and the other related technologies (DoDD, 1988).

3. Embedded Systems

An embedded system is a microprocessor system in which the computer is completely encapsulated by or dedicated device or system it controls. Unlike general purpose computers such as personal computer, an embedded system performs a set of predetermined tasks and specific requirements. Since the system is dedicated to specific tasks by engineering can optimize the design reducing its size, computing resources, product cost and energy consumption. The embedded systems ranging from: smartcards, mobile phones, PDAs, avionics systems, routers, hubs, switches, firewalls, washing machines, TV, tractors and farm implements. Historically, the first embedded system recognized was the Apollo Guidance Computer developed by Charles Stark Draper at MIT in 1970. The computer guide, operating in real time, the item was considered more risky than the Apollo project reported (Morgan, O'Connor, & Hoag, 1999). The software written for embedded systems is most often called firmware, and stored in a ROM or flash memory. Sometimes the system also runs with computational resources limited: no keyboard, no screen, and with little memory.

Design Issues for Embedded Systems

A major problem of the mobile equipment is power consumption. These devices have little computing power (processor speed and limited storage space). Due to constraints of cost, size and battery power, embedded systems projects take into account such limitations in the design and requirements analysis, especially as to the question of security (Ramesh & Piyush, 2002).

The algorithm chosen to implement the encryption has to be efficient and optimized, suitable for storage with little memory. These cryptographic algorithms contains many loops and many variable assignments, which consumes much current in the memory storage, the designers do not have the freedom to implement a security computationally very strong. It is a decision between cost and performance (Berkes, 2006). In chip manufacturing production costs are directly related to the amount of functions that the project has established, then for any function that is small has a great impact on production of million units per year. Most existing on the market microcontrollers are 8-bit, which cannot store an encryption key managing large. This can make it very expensive development, impossible to be practical in applications loaded, for example. The hiring of certain parts or subsystems

of a software project aimed at reducing costs internally enjoying the "know how" and expertise of freelance engineers, small teams or even small businesses to write a few kilobytes of code per year. These companies often cannot afford a security expert and often do not realize they need one, but apparently simple programs may need to provide some level of security assurance.

Strategies Security Risk in Flash Memory

The National Institute of Standards and Technology (NIST) announced in December 2011 the launch of public recommendations "Special Publication" Draft SP 800-155, with guidelines for measuring the integrity of the Basic Input Output System - BIOS. This document describes the security components and their basic guidelines necessary to establish a safe system of measurement integrity. Due to its unique and privileged position within the architecture of the computer BIOS is a critical component of security systems, if you're lacking security, outdated, or corrupted by the presence of malware (malicious code), you can allow or be part of a sophisticated attack, directed by an organization or a permanent denial of service (DoS) (NIST, 2011). The guidelines contained herein are intended to facilitate the development of products that can detect problems with the BIOS so that organizations can take appropriate corrective actions to prevent or limit damage. This publication focuses on the safety properties of products and capabilities to measure the integrity of the BIOS, will also provide security administrators in organizations a better understanding of the assurances that these types of products can provide, and the procedures to be integrated into systems and management processes (NIST, 2011).

4. Attacks on Embedded Systems

Security issues for embedded systems is not new. In 2001 was reported in an article that was carried out a series of phone calls to certain prefixes: 408 (San Jose), 415 (San Francisco), 650 (Silicon Valley), and 510 (Berkeley), concentrating more on the prefixes 415 and 510 and thousands initial from 0000 to 9999. These routes has been found that a modem deprotected controlling a transmission power high voltage, the modem answered the call, however, did not perform any action and there have proved that these security systems (Shipley & Simson, 2001). There is a wide variety of attacks on embedded systems failures, which exploit a hardware failure (an unexpected condition or defect) that leads to a processing error that is beneficial to the attacker (Anderson, Bond, Clulow & Skorobogatov, 2006). Attacks failure may overlap with physical tampering. Methods of inducing faults include the provision of noise or different clock signals, incorrect voltage, over temperature, radiation or high energy beams such as UV rays, laser, among others for example (Berkes, 2006; Eric, Standaert & Quisquater, 2007).

Embedded System with FPGA

The re-configurable computing is still a developing area, unlike other computer architectures in which the concepts have already been extensively debated, tested and proven. So look for new concepts of re-configurable computing, define them and validate them is a challenge for researchers. There are several fields of application of knowledge in Field Programmable Gate Array - FPGA: aviation, telecommunications, radar, medicine, robotics, automation, alarms and encryption, among others. With this technological support, it is possible to develop projects using processor components programmable logic FPGA or CPLD - Complex Programmable Logic Devices. The widespread use of processors focuses on electro / electronics for everyday use, are circuits that comes embedded in equipment, for example, phones, cars, watches, PDA's (Personal Digital Assistant). These devices leave the factory, with their pre-defined features. From this, then there is a new category of hardware, the re-configurable, which have their functionality defined by users and not just those implemented by the manufacturers. In this context, one can cite the FPGA as a solution. In this sense a family of FPGA can contain between Several million flip-flops that can be programmed to perform different types of flash memory storage (XILINX, 2009). The next section will describe the motivation of this work.

Protection of Embedded System with FPGA

One of the reasons that motivated this work is the large number of counterfeit products, which are placed adulterated to the consumer that is the result of a modern type of theft crime called piracy. As reported, these products threaten the survival of companies and has a strong impact on the global economy. Importantly, there is no unbreakable security. Ultimately, there is nothing you can do to completely protect your project a certain type of attack. If someone wants your data or your project, they can use brute force techniques to achieve your goal. This is not a single striker, casual, but possibly a government or a competitor that can fund research for this purpose. For that reason, you are creating a solution that adequately protect the most common threats (XILINX, 2009 & 2011). When deciding on what level of security to be used in the project, it becomes necessary to assess their security needs the cost of the product versus the system security (Ramesh & Piyush, 2002).

This is an assessment that you need to do and after this analysis it is possible to determine which set of security you can use. There are a variety of solutions available from Xilinx which can exploit to solve the problem of simple to complex using FPGAs Xilinx Spartan ®-3A/AN and Virtex-5/6 ®, which can help protect your profits products and intellectual property (XILINX, 2009 & 2011).The FPGA Xilinx family offers three security levels as follows Safety Levels Description: Standard. Unrestricted access to all setup functions and two-way reading, level 01: disable all the functions of reading for both bi-directional configuration or JTAG ports (pins external). Is only allowed to read through the bidirectional ICAP, in the level 02 disables all operations in all reading bidirectional ports and level 03 disable all the functions of setting and reading of all bidirectionals ports configuration the of JTAG. The only command that may be issued and executed at this level is the reboot that erases

the device configuration. A further safety mechanism on the platform of the FPGA using two identification numbers (ID), and the device is a DNA with 57 Bits and the other located in the flash memory with 64 Bits. The two IDs are unique, resulting in a much larger number of combinations therefore drastically increases the time required to break the security algorithm (XILINX, 2009 & 2011). The project is specifically linked to both. The third mechanism is stored in the verification code. The security code can be stored in a chip inside the own FPGA is a field defined safety record, see page 8 schematic. This allows the security system is self-contained, without need of external interfaces or storage (XILINX, 2009). This feature increases the overall security and makes it harder for someone to reverse engineer their product.

5. Protecting intellectual property (IP)

Among the various types of security distinguishes itself the mechanism for implementation of Authentication Device Number (ID) - DNA, an authenticator that is unique, individual, private deck Xilinx. Authentication solves a number of key concern for designers to IP allowing them to protect the project from unauthorized copying. Furthermore, the use of the device provides complete traceability DNA, allowing a designer FPGA can monitor shipments of units for a particular customer in order to manage your project and financial part (XILINX, 2009).

6. Methodology and Tests

It was used in our research, development platforms: Spartan-3A/3AN, Virtex-6 and set of software: ISE Project Navigator, IMPACT, Time Analyzer version 11.1 and lap-top Acer Extensa 4420 4Gb, where he held a series of tests, monitoring of current sources feeding the core processor and memory banks 0, 1, 2 and 3 FPGA DDR2 SDRAM (DS529, 2010).The values were obtained from the loads generated when submitted to different levels of security and finally using the cryptographic algorithm RC4 with several key sizes. It also collected the runtime in order to observe the impact and behavior in terms of FPGA power consumption.

7. Experimental Results

The table 1, show the measures collected in accordance with standard features (current mA.) can be concluded that to implement a security level the impact is not significant and FPGA platforms that can help protect your projects from the use of resources security levels that allow you to join their project to a particular feature, projecting the most likely security threats. Another result observed in the table: 2, and figures 2 and 3, was the response in terms of total current and response time the FPGA when subjected to a load generated by the RC-4 algorithm with different size keys conclude also that the developer must

seek the best encryption algorithm that meets the requirements of the project. There are several manufacturers of FPGA: Xilinx, Altera, Actel, Digilent, Lattice Semiconductor and Atmel. Researchers should seek the best features that meet the conditions of the analysis requirements of the project taking into consideration the state of the art. This work can verify that it is possible depending on the project to deploy a security policy with very low cost was that the results showed.

Table 1. Measuring Current in FPGA

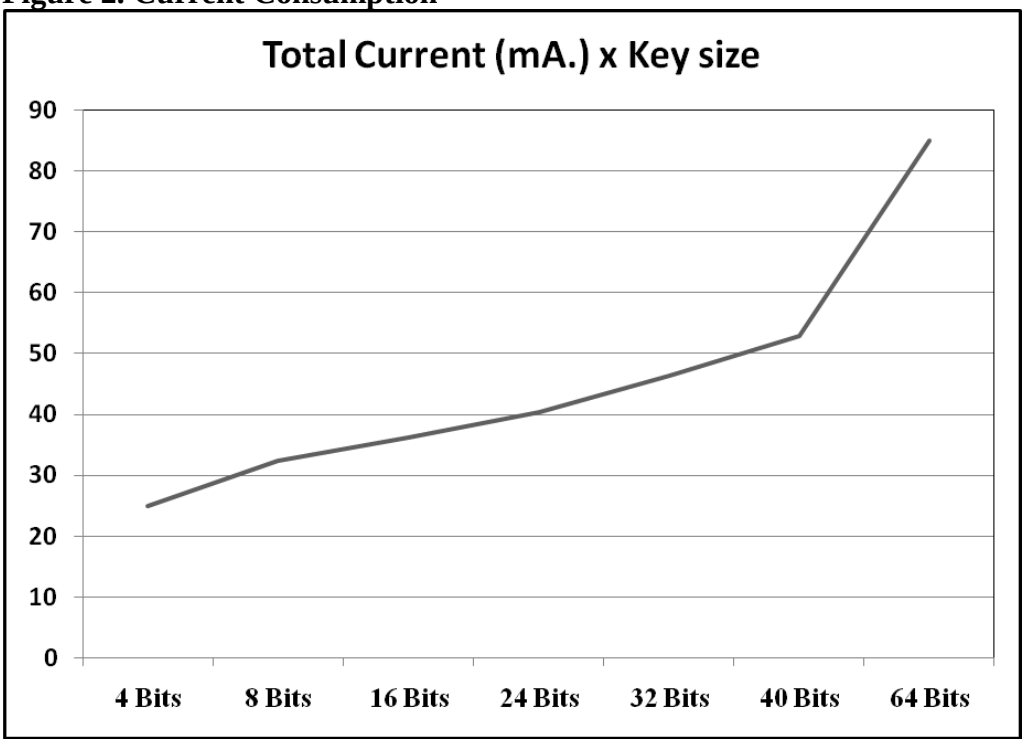
Security Level	Current (mA) - Power Supply to FPGA				Time Load
	Core vcc aux.	Core vcc int.	Bank 0,1, 2 DDR2 SDRAM	Bank 3 DDR2 SDRAM	
Default	9,8	9,0	90,	-	-
Level 01	10,0	9,2	90,	-	-
Level 02	10,0	9,4	90,	-	-
Level 03	10,3	9,6	90,	-	-
Bitstream 334 Kb	18,0	28,3	161,0	20,0	110 ms.
Read DNA	14,0	12,7	166,0	8,3	-
Bitstream 134 Kb Compressed/Encrypted .	30,0	45,5	183,7	35,0	80 ms.

Table 2. Measuring Total Current and Execution Time in RC4 code

Algorithm	RC4						
Key size Bits	4	8	16	24	32	40	64
Execution Time (sec)	0,330	0,600	0,950	1,89	2,64	2,89	5,45
Total Current (mA)	25	32,4	36,2	40,4	46,3	53.0	85

Figure 1. Execution Time

Figure 2. Current Consumption



Bibliography

BSA, (2010). 'Piracy Impact Study: the economic Benefits of reducing software piracy'. Available at http://portal.bsa.org/piracyimpact2010/index. html [20 april 2011]

XILINX. (2009). 'Spartan-3 Generation Configuration User Guide Extended Spartan-3A, Spartan-3E, and Spartan-3 FPGA Families'. Available at www.xilinx.com/ support/documentation/user_guides/ug332.pdf [10 december 2011]

XILINX (2011). 'Virtex-6 FPGA Configuration User Guide'. Available at http://www.xilinx.com/support/documentation/user_guides/ug360.pdf [03 sSeptember 2011].

Berkes J. (2006). 'Hardware Attacks on Cryptographic Devices Implementation Attacks on Embedded Systems and Other Portable Hardware'. University of Waterloo Prepared for ECE 628. Available at http://www.sysdesig.ca
/archive/berkes_hardware_attacks.pdf [15 January 2012].

Shipley P. & Simson L. G. (2001). 'An Analysis of Dial-Up Modems and Vulnerabilities', Spring. Available at http://www2.dis.org/
filez/Wardial_ShipleyGarfinkel.pdf [21 January 2012].

Eric P, Standaert, F. X, & Quisquater, J. J. (2007). 'Power and Electromagnetic Analysis: Improved Model, Consequences and Comparisons'. Available at http://dl.acm.org/citation.cfm?id=1232257.1232265 [21 January 2012].

NIST, (2011). 'Bios Integrity Measurement Guidelines (DRAFT SP 800-155)' Available at http://csrc.nist.gov/publications/PubsDrafts.html [21 january 2012].

Morgan. C., O'Connor. J. & Hoag D. (1999). 'Draper at 25 Innovation for the 21st Century'. Available at http://www.draper.com/Documents/draperat25.pdf [21 January 2012].

Ramesh, K, Piyush, M. (2002). 'Minimizing Energy Consumption of Segure Wireless Session With QOS Constraints'. Available at http://ieeexplore.ieee.org/ [24 march 2012]

Anderson, R. Bond, M. Clulow, J. & Skorobogatov. S. (2006). 'Cryptographic Processors-A Survey'. Available at http://ieeexplo
re.ieee.org/ [08 October 2011].

DS529, (2010). *Data* Sheet Spartan-3A FPGA Family: Pinout Descriptions. Available at http://www.xilinx.com/support/documentation/data_sheets/ds529.pdf
[10 December 2011].

DoDD, (1988). 'Security Requirements for Automated Information Systems (AISs)'. Available at http://csrc.nist.gov/gro
ups/SMA/fasp/documents/c&a/DLABSP/d520028p.pdf [21 August 2011].