Firmware Protection and Attacks Against the ATMega Microcontroller Series

Dionisio Perez-Mavrogenis

February 15, 2014

Abstract

Give paper topic, objectives and conclusions reached.

1 Introduction

mention abbreviation mcu=microcontroller unit

1.1 Problem Statement

Perhaps need to classify attackers : e.g. home hacker ¡¡ crackers ¡¡ funded organisations

1.2 Objectives of Paper

2 The ATMega MCU Series

2.1 Predecessors

predecessors to the atmega and what was wrong with them?

2.2 ATMega Architecture and Series Improvements

ATmega644 is harvard architecture [AtmelCorporation(2012)]

2.3 ATMega Architecture and Security Features

3 Current Attacks

* attack types * budget * how the ATMegas fail

4 Counter Meassures to known attacks

* overview of most popular techniques (tamper resistance, crypto-units etc) * how they improve security * cost breakdown

5 Securing the mega

5.1 Motivation

5.2 Current Attack Vectors

5.3 Protective Steps

* feasible? * added cost (in terms of $$, extra hardware and software implementation penalties/overhead)

6 Evaluation

6.1 Solutions overview

6.2 conclusions

References

[AtmelCorporation(2012)] AtmelCorporation. *Atmel ATmega644 data sheet*, 2012. URL

http://www.atmel.com/Images/doc2593.pdf.