Research in Firmware Security

Svetoslav Stoyanov

October 23, 2020

Abstract

In recent years embedded devices have become very popular in many countries worldwide, they are often used in households, factories, and even in infrastructure objects. Their usage is predicted to increase steadily in the next decades. Our focus is that all embedded devices run on Firmware, which is basically computer software that is meant to work with specific hardware. The Firmware is not as secure as we would like it to be, there are many ways of hacking (reverse engineering) it so that one (the hacker) can find how exactly it operates and if there are any holes that can be exploited for benefit or used to harm either the users or the creators of the firmware.

0.1 Introduction

The research we are conducting is about firmware security mainly but we will touch on the topic of embedded devices also because the two work together. In general, most devices with firmware are relatively easy to reverse engineer by hackers who want to find vulnerabilities that they can exploit to attack different parts of the eco-system. Therefore the goal of this research is to find a way to increase firmware security.

0.2 Research Design

0.2.1 Purpose of the study

The goal of the study is to find out how exactly is firmware being reverse engineered in order to find new protection methods against reverse engineering.

1. The first thing is to understand how is firmware being reverse engineered?
    - What tools an techniques are used?
    - How does those tools work, what algorithms they execute?
    - Also the result is very important, what holes are found?
    - How dangerous are those they?
    - Can those holes be used to help access other parts of an software eco-system?
2. Simple ways to enhance firmware security (if any):
    - Are there any software solutions to patch known vulnerabilities?
    - Are there any hardware solutions to patch known vulnerabilities?
    - How to implement those solutions?
    - Any other ways for improving security?
3. Applied solutions result check:
    - Does the applied software solution work?
    - Does it creates any other issues?
    - Does the applied hardware solutions work?
    - Do they create any other issues?
    - How much harder is now to penetrate firmware's code after applying the discovered solutions?
    - Does the number of reverse engineered and penetrated devices decrease after applying the discovered solutions??
    - Does the proposed solutions worth the effort for the achieved result?

0.2.2 Data types

The collected data can be both qualitative and quantitative even though, we mainly rely on qualitative data. Quantitative data is only used to compare numbers and statistics and derive results in numeric or other forms.

- Observation Data
- Derived/Compiled Data

0.2.3 Methods of data collection and analysis

1. Pick the most suitable and proven literature about the subject.
2. Find cyber security experts published opinions.
3. Read papers about disclosed reverse engineering of embedded devices cases.
4. Find existing solutions with potential of improvement.

0.2.4 Sources

The sources of information can be books(any type), websites, other research papers and articles but they must be authentic and with proven validity.

0.2.5 Strategies

The strategy of how this research must be conducted is to seek answers to the questions mentioned in "Purpose of the study" subsection. The questions shall be answered by reading previous researches on very close to this subjects. We will try to collect material proving that there are ways to improve security in firmware and to restrict or block reverse engineering of embedded devices. That evidence should not have been determined previously in order to be valid for this research.

0.2.6 Hypothesis

Providing even a minor solution regarding increase security for reverse engineering of embedded devices and their firmware, may result in rapid decrease in exploits of embedded devices therefore companies shall spend less on security and more on functionality.