Applied Research in Firmware security of embedded devices

Jan Polfers and Svetoslav Stoyanov

November 30th 2020
Module: SEAR
Venlo, Limburg, Netherlands

Abstract

- Complete, but very succinct summary of the paper
- Half a page long
- Short description of research(brief statements of the purpose, methods, results and conclusions)

Contents

List of Figures

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 software eco-system. Therefore the goal of this research is to find a way to increase firmware security.

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. The firmware used in all embedded devices is basically computer software that is meant to work with specific hardware in order to execute one or a few very concrete functions. The Firmware is not as secure as we would like it to be, there are many ways of hacking (breaching) 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. Even though there are many ways of hacking an embedded device, the focus of this research paper is mainly on binary reverse engineering in a firmware context. Reverse engineering is the process by which an artificial object is deconstructed to reveal its designs, architecture, code or to extract knowledge from the object. The point of reverse engineering a device is to reach the firmware.

"A firmware is a program or set of instructions programmed on a hardware device(embedded device) which provides the necessary instructions for how the device communicates with the other computer hardware. For the purpose to be programmed on a hardware, the firmware is usually stored in the flash ROM of a device. While ROM is "read-only" memory, the flash ROM can be erased and rewritten because it is actually a type of flash memory. Firmware can be thought of as "semi-permanent" since it remains the same unless it is updated by a firmware updater." (Christensson, Per, 2020) Anyway an attacker can also modify the firmware and inject it back on the device replacing the old firmware with new corrupted firmware code.

The physical objects containing firmware (embedded devices) and connected to a network are described by the term "Internet Of Things".

Although IEEE IoT Initiative is proceeding to draft a white paper (Roberto Minerva, 27 May 2015) for the formal definition of IoT, there are still no common agreements for the definition of IoT. In this article, we define a "Thing" on IoT that indicates a physical or virtual object which connects to the Internet and has the ability to communicate with human users or other objects. Along with the growth of IoT, new security issues arise while traditional security issues become more severe. The main reasons are the heterogeneity and the large scale of the objects. The impact factors can be further divided into two categories: the diversity of the "Things" and the communication of the "Things". It is divided into two categories given that each of the category encounters different security problems. First, the security problem for the "Things" is created by vulnerabilities produced by careless program design; this creates opportunities for malwares or backdoors installation. Based on the heterogeneity

and the scale of the "Things" in IoT, such security problems are more complex compared to the security problems that we have faced now. As for the communication medium of the "Things", it is expected that the networking environment for IoT will be heterogeneous. Various communication media may face different security challenges. Overlooking these security problems will compromise the availability of the "Things". As for the contents of the communication, the heterogeneous data structure and protocols also make content protection more complex
//IOT Detailed explanation As mentioned before, the usage of embedded devices in households, factories, infrastructure objects is increasing and is
//Why this is important but (IOT, machines in factorys etc.) it is included. More details and make sure the reader is aware of the importance of the security. Because it can affect everything.

- Provide the reader with everything they need to know to understand what you are doing and why
- Length: max 3 pages
- Theoretical background (literature review)
- Why the work is important
- Specific research question
- (if applicable) Hypothesis to be tested
- Divide into subsections

2 Methods

- How you performed the experiment / interview / survey or how you set up your comparative analysis
- Length: min. 2 pages
- Methodology (Research strategy, material, planning): which method you used, why, how it was carried out
- NO results or interpretation in this section!

We should primarily focus on experiments and research papers as material. Because these two sources give us a deep understanding of the underlying structure and the causes of the problem. Every paper you read should be logged on one of the following pages. To prove our research we maybe provide interviews.

3 Results

Topics: 1. Reverse engineering in general introduction Half a page or a page about it in general and methods against it
2. Differences in reverse engineering between java c++ and binarys Maybe own chapter or just half a page I dont know Why methods applied for java or c++ cant be applied for binarys
3. Reverse engineering of binaries automated and non automated (Manual and binwalk) This is used as an introduction into binary reverse engineering
4. Methods against reverse engineering binarys Explain a list of methods to prevent reverse engineering.
5. Obfuscation methods Old and reliable methods and state of the art
6. Deobfuscation methods Old and reliable methods and state of the art

- Share the data you found
- Length: min. 2 pages
- Describe the results (do NOT add your interpretation/analysis)
- Graphs, figures and tables that show your data belong in this section. Describe the graphs and explain what the reader is seeing

4 Discussion

- Interpret the results from the previous section
- Answer your research question/s and explain if your hypothesis was proven right or not: Refer to starting point (objective research question)
- Length: max. 4 pages
- Evaluate process (Reflection: how did it go)
- Further research (how your research could be improved, what else could be done)