# Research in " How to increase firmware security? "

Svetoslav Stoyanov
Software Engineering
Fontys Venlo Hogeschool

30/10/2020

# Contents

# Chapter 1

# Introduction

## 1.1 Research Design

The conducted research is mainly about firmware security but the topic of embedded devices will also be mentioned because the two work together. An embedded device is an object that contains a special-purpose computing system. The system, which is completely enclosed by the object, may or may not be connected to the internet. Embedded devices are something usual for many households and their number is expected to greatly increase in the next few years. Because of that they have lately become the usual target for security breaches. If an attacker manages to access an embedded device's firmware (source code) he can then exploit other parts of the software ecosystem. For the needs of the research the history of hacking of firmware shall be reviewed. Hacking can be achieved with different approaches like reverse engineering of an embedded device or

### 1.1.1 Purpose of the study

The goal of this research is to find a way to better protect embedded devices' firmware code from being accessed or edited by unauthorized entities, since it is the weakest point in an embedded device (Andrei Costin).

# Chapter 2

# References

https://doi.org/10.3390/app10114015 - College of Computer, National University of Defense Technology, Changsha 410073, China* Author to whom correspondence should be addressed. Appl. Sci. 2020, 10(11), 4015; Received: 10 April 2020 / Revised: 5 June 2020 / Accepted: 8 June 2020 / Published: 10 June 2020

www.link-springer-com.fontys.idm.oclc.org/chapter/10.1007

www.s3.eurecom.fr/docs/bh13us_zaddach.pdf

http://ojs.unsysdigital.com/index.php/ijrm/article/view/889 - Hafez Fouad," Embedded System Design of Remote Healthcare Monitoring Center using Web-Technology ", International Journal of Robotics and Mechatronics IJRM, Vol.2, Issue 2, Derby University, UK, Dec. 2015.