

Research in ” How to increase firmware security? ”

Svetoslav Stoyanov  
Software Engineering  
Fontys Venlo Hogeschool

30/10/2020

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Research Design . . . . .	2
1.1.1	Purpose of the study . . . . .	2
<b>2</b>	<b>References</b>	<b>3</b>

# 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. 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 exploit that access in order to exploit other parts of the eco system.

#### 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

College of Computer, National University of Defense Technology, Changsha 410073, China\*

Author to whom correspondence should be addressed.

Appl. Sci. 2020, 10(11), 4015; <https://doi.org/10.3390/app10114015>

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](http://www.link-springer-com.fontys.idm.oclc.org/chapter/10.1007)

[www.s3.eurecom.fr/docs/bh13us\\_zaddach.pdf](http://www.s3.eurecom.fr/docs/bh13us_zaddach.pdf)