Research in Firmware Security

Stoyanov

October 3, 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

0.3 Data collection

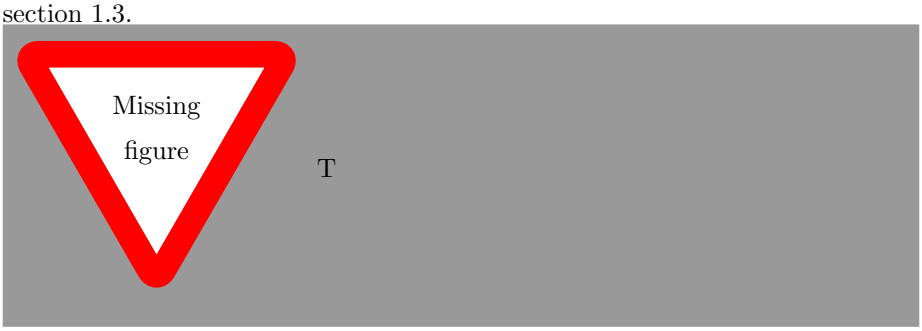
0.4 Analysis

Make a cake . . .

c

zastrelqi indieca

, Make a cake . . . which renders like. The ommand has this structure: . The todo text is the text that will be shown in the todonote and in the list of todos. The optional argument options, allows the user to customize the appearance of the inserted todonotes. For a description of all the options see section 1.3.



T

he

c

ommand inserts an image containing an attention sign and the given text. The command takes only one argument

htexti

, a text string that could describe what the figure should consist of. An example of its usage could be

Make a sketch of the structure of a trebuchet.