The Bad Program

The subtitle

Shiva Prasad Gyawali, Shirinshoev Azamat

27 November 2024

1 Introduction

2 Options Legacy version

In this, we explored the various options that might have been used to compile our original door-locker binary. The compilation flags we will put into `LEGCFLAGS=` and the linker flags we will put`LEGLDFRLAGS=`.

2.1 Compilation options (LEGCFLAGS)

2.1.1 `-fno-stack-protector`

With the use of checksec tool, we saw that the provided `door-locker` binary doesn't have the canary. Thus, we assume that the flags `-fno-stack-protector` must have been used.

2.1.2

Explain here possible options, and what each options do… Also explain, what options should be removed and how it enhance security…

2.2 LEGLDHLAGS

Explain the possible options, and explain what each otpions do.

3 Identified threats and their mitigation

In this section, we will try to implement the mitigations we proposed in previous report.

3.1 Mitigations for Buffor overflow

3.2 Mitigations for visibility of Sensitive function

3.3 alternative of 'strtol'

3.4 Improved user feedback and error message

4 Recommendation for future processes

In this section, we will propose some improvements/feedbacks to