UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO DI INFORMATICA

Corso di Laurea in
Sicurezza dei Sistemi e delle Reti Informatiche

Security Fuzzing of ADS-B, NextGen protocols and avionics devices

RELATORE
Dott. Valerio Bellandi

TESI DI LAUREA DI
Giulio Ginesi
Matr. 872795

Anno Accademico 2017/2018

Ai miei genitori

Ringraziamenti

Contents

Chapter 1

Introduction

The rest of the thesis is organized as follows:

- *Chapter 2: Avonics Protocols*
  In this first chapter I will present the basics of some common Protocols.
- *Chapter 3: Fuzzing*
  In this chapter will be presented the principles and ideas behind *Fuzzing* as well as some common techniques.
- *Chapter 4:*
- *Chapter 5:*
- *Chapter 6:*
- *Chapter 7:*

Chapter 2

Aviation Protocols

Chapter 3

Fuzzing

3.1 Brief History

The term Fuzz Testing was first introduced in 1988 when three students from University of Wisconsin-Madison proposed a tool to test the behavior of UNIX Utilities when given unexpected random characters as input. [1] Those first tools where pretty simple and as it can be easily imagined they just generated random strings. However the findings where impressive: 25-30% of the tested utilities crashed when tested with the new tools. For this reason fuzz testing begin to gain more and more popularity until the first years of 2000 when it grow at the point that it become a filed of research and engineering.

This initial fuzzing technique is known as `Black Box Fuzzing`.

Getting closer to the present day more and more techniques for fuzz testing emerged, I will illustrate some of those in the following sections:

3.2 White Box Fuzzing

This is a more sophisticated fuzzing technique, compared to the `Black Box Fuzzing`

Chapter 4

Experimental Setup

Chapter 5

Results Analysis And Conclusions

Chapter 6

Future Work

Bibliography

[1] Bryan So Barton P. Miller Lars Fredriksen. “An Empirical Study of the Reliability of UNIX Utilities”. In: (1990). URL: ftp://ftp.cs.wisc.edu/paradyn/technical_papers/fuzz.pdf.