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

T0D0 1: Short introduction

The rest of the thesis is organized as follows:

T0D0 2:

- *Chapter 2: Avonics Protocols*

- *Chapter 3: Fuzzing*

- *Chapter 4:*

- *Chapter 5:*

- *Chapter 6:*

- *Chapter 7:*

Chapter 2

Software testing and Fuzzing

T0D0 3: maybe put some references about fuzzing hystory and actual world, just few lines.

2.1 Software testing methods

T0D0 4: explain software testing techniques (white, black, gray box)

2.2 The fuzzing world

"Fuzzing is the process of sending intentionally invalid data to a product in the hopes of triggering an error condition or fault."[1]

T0D0 5: explain how a fuzzer works and how the previous methods applies to the fuzzing world. Also explain fuzzing approaches.

2.3 State of the art

T0D0 6: describe afl, afl-unicorn and peach.

Chapter 3

Avionics Protocols

3.1 OldGen

T0D0 7: explain how 1090mhz protocols works

3.2 NextGen

T0D0 8: explain how 978/nexrad/tis-b/fis-b protocols works

T0D0 9: maybe explain backwards compatibility with 1090 using 1090ES (extendes squitter) also put the theory about using fis-b tis-b in 1090mhz band. (Find some references and obtain some documents FREE)

Chapter 4

Experimental Setup

4.1 Hardware Setup

T0D0 10: Describe the hardware used, why we used that hardware and why it can be usefull to test also on such a hardware. Getting dedicated hw is difficult and expensive. This part is explained really well in the paper. copia and migliora.

4.2 Software Setup

T0D0 11: Explain why we used what we used. Same as before, copy from paper and final report.

4.3 Proceedings

T0D0 12: maybe we don’t need this

Chapter 5

Results Analysis And Conclusions

5.1 Caveats

T0D0 13: Put all the problems we had here

5.2 Results

T0D0 14: Put the significative Results here and the state of the fuzzers

5.3 Conclusions

T0D0 15: I can think about doing a separate chapter for the conclusion

Chapter 6

Future Work

T0D0 16: Future work and proprietary fuzzer developement

Bibliography

[1] Pedram Amini Michael Sutton Adam Greene. *Fuzzing: Brute force vulnerability discovery*. Addison Wesley, 2007.