PhD Thesis Examination Report – Part 1

Name of Student: Hongxu CHEN

Thesis Title: SECURING SOFTWARE SYSTEMS VIA FUZZ TESTING AND VERIFICATION

Conclusion and Recommendation/Comment

The Ph. D. candidate has published:

1. Three international conference papers as first author
2. One international conference paper as co-author
3. One international journal paper as co-author

The submitted thesis is well-written, and the structure of the thesis is well-organized. I only have some suggestions. Detailed comments can be found in the following.

Summary of the Thesis and Detailed Evaluation

Chapter 1:

This first chapter describes the motivations and the challenges, and then summarizes the contributions of this thesis.

Detailed Comments:

(1) On p. 1, in the first line in Section 1.1, "… vulnerabilities and weakness." should be "… vulnerabilities and weaknesses.". This problem occurs in line 8 in the same paragraph as well.

(2) On p. 1, in line 12 of Section 1.1, "153 lives were lives were lost during this accident, including 149 passengers and 8 crew". The numbers do not seem to match. Do you mean 158?

(3) The chapter numbering in Figure 1.1 is not correct. There is no Chapter 8. It seems that there is one chapter shifting.

(4) In line 9 on p. 4, "It is configurable in that it …" should be "It is configurable in the sense that it …". This problem occurs in line 11 on the same page.

Chapter 2:

This chapter introduces the background knowledge about Greybox Fuzz Testing, type systems, and verification based on type systems.

Chapter 3:

In this chapter, a novel directed greybox fuzzer, HAWKEYE, is proposed. HAWKEYE combines static analysis and dynamic fuzzing, based on four desired properties. HAWKEYE is equipped with a better evaluation of the distance between input execution traces and the user specified target locations such that the target locations can be reached faster than existing state-of-the-art greybox fuzzers. Experiments show that HAWKEYE is effective in patch testing, crash exposure, and other analysis scenarios.

Detailed Comments:

(1) Are AFL and AFLGo the same tool? In this chapter, sometimes AFL is mentioned, while sometimes AFLGo is mentioned. Please clarify.

(2) The fonts in Figure 3.3 are too small to be recognized.

(3) In the last paragraph on p. 23, what is the exact distance formula defined in AFLGo? From the examples, I cannot deduce the distance formula. Considering a Ph.D. thesis is supposed to be self-contained, I would suggest the author give the exact distance formula. In addition, I suppose “abcdTZ” is a trace. Why not use the same notation <abcdTZ>? That is, $d_s(<abcdTZ>)$?

(4) On p. 28, the figure numberings in lines 5 and 6 in Section 3.4.2 seems inconsistent to Figure 3.4. It should be Figure 3.4(A), instead of Figure 3.4a. Similarly, it should be Figure 3.4(B), instead of Figure 3.4b.

(5) On pp. 28-29, in the two points (1) and (2), the factor functions Φ and Psi are defined. Why are the two constants ϕ and ψ usually to be 2, respectively? What exactly do these functions and constants mean? Please clarify.

(6) On pp. 28-29, in the two points (1) and (2), two terms C_N and C_B are introduced. In the factor function definitions, they seem to be non-functions. However, in the second paragraph (reversed order) on p. 29, they are used like functions. Please refine the notations.

(7) All the equations defined in this chapter are too small. Please use the normal size.

Chapter 4:

In this chapter, a greybox fuzzer, DOUBLADE, is proposed for testing multithreaded programs. The core of DOUBLADE is a thread-aware seed generation technique that produces valuable seeds to test the multithreading context. DOUBLADE performs three categories of instrumentations guided by static analysis to explore new program paths that are relevant to thread-interleavings. Based on the additional feedback provided by these instrumentations, a series of dynamic strategies are applied for exercising thread-interleaving related paths and generating multithreading relevant seeds. The dynamic strategies are hereby optimized for the feedback provided by these instrumentations to improve the effectiveness of fuzzing. The experimental results show that DOUBLADE significantly outperforms the state-of-the-art greybox fuzzer AFL in generating multithreading relevant seeds, detecting multithreading relevant vulnerabilities, and exposing concurrency bugs via generated seeds.

Detailed Comments:

(1) Line 3 (reversed order) on p. 52, "… it executes func_1 otherwise func_2; …" should be "… it executes func 1; otherwise, func 2; …".

(2) Line 3 in Section 4.2.1 on p. 55, ". if the check fails, …" should be ". If the check fails, …".

(3) In the second paragraph of Section 4.2.2, it should be Figure 4.2(B), instead of Figure 4.2b.

(4) The fonts in Figure 4.2 are too small.

(5) The fonts in Figure 4.3 are too small.

(6) On p. 62, why is P_{s0} set 0.5 empirically? What is the rational behind? Please clarify.

(7) On p. 63, why is the default value of P_{m0} 0.33?

(8) All the equations defined in this chapter are too small. Please use the normal size.

Chapter 5:

In this chapter, a fuzzing framework, *Fuzzing Orchestration Toolkit* (FOT), is proposed. FOT is a general greybox fuzzing framework, which aims to reuse, integrate and evaluate fuzzing extensions as well as try new techniques. The design of FOT brings three advantages: versatility, configurability, and extensibility.

Chapter 6:

In this chapter, a precise and lightweight type system is proposed for featuring Android permission model that enforces secure information flow in an imperative language. The soundness (in terms of non-interference) of the type system is proved. Compared to existing work, the proposed type system can specify a broader range of security policies, including non-monotonic ones. A decidable type inference algorithm is also proposed, which reduces the original problem to a constraint solving problem.

Detailed Comments:

(1) On p. 96, the grammar definition is too small. Please use bigger sizes.

(2) The fonts in Figure 6.1 are too small. Please use the normal size.

(3) The formulas defined in Definition 6.10 are too small. Please use bigger sizes.

(4) The fonts in Figure 6.2 are too small. Please use bigger sizes (maybe rearranging the rules is also needed).

(5) The fonts in Figure 6.5 are too small. Please use bigger sizes (maybe rearranging the rules is also needed).

(6) The fonts in Figure 6.6 are too small. Please use bigger sizes (maybe rearranging the rules is also needed).

Chapter 7:

This chapter concludes the thesis and summarizes all the works included in the thesis.