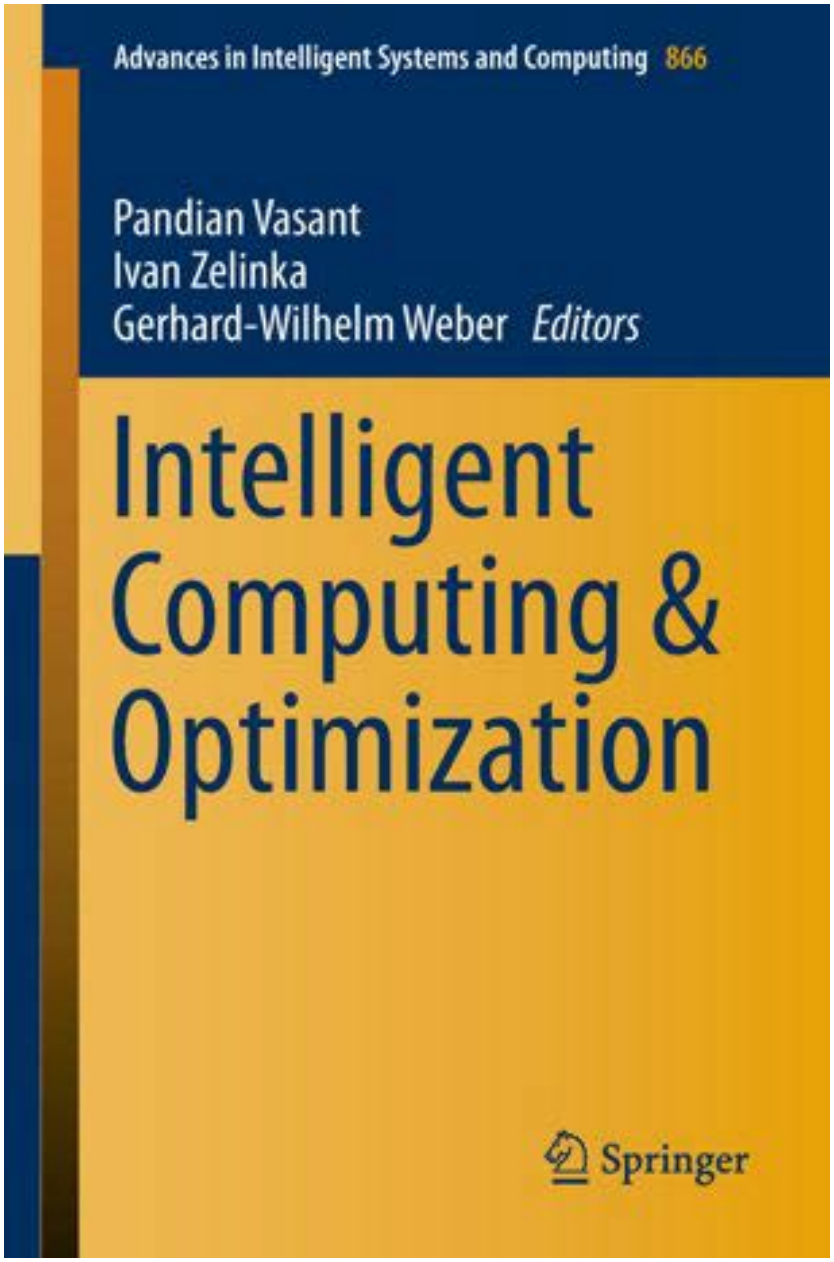

Intelligent Computing & Optimization

Editors: Vasant, Pandian, Zelinka, Ivan, Weber, Gerhard-Wilhelm (Eds.)

ISSN 2194-5357 ISSN 2194-5365 (electronic)
Advances in Intelligent Systems and Computing
ISBN 978-3-030-00978-6 ISBN 978-3-030-00979-3 (eBook)
https://doi.org/10.1007/978-3-030-00979-3

Library of Congress Control Number: 2018955576

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

Fuzz Test Case Generation for Penetration Testing in Mobile Cloud Computing Applications

Ahmad Salah Al-Ahmad[1] and Hasan Kahtan[2(✉)]

[1] Department of Computer Science, Universiti Teknologi, Mara, Malaysia
ahmad.salah.85@gmail.com
[2] Department of Software Engineering, Faculty of Computer Systems and Software Engineering, Universiti Malaysia Pahang (UMP), Lebuhraya Tun Razak, Gambang, 26300 Kuantan, Pahang, Malaysia
hasankahtan@ump.edu.my

Abstract. Security testing for applications is a critical practice used to protect data and users. Penetration testing is particularly important, and test case generation is one of its critical phases. In test case generation, the testers need to ensure that as many execution paths as possible are covered by using a set of test cases. Multiple models and techniques have been proposed to generate test cases for software penetration testing. These techniques include fuzz test case generation, which has been implemented in multiple forms. This work critically reviews different models and techniques used for fuzz test case generation and identifies strengths and limitations associated with each implementation and proposal. Reviewing results showed that previous test case generation methods disregard offloading parameters when generating test case sets. This paper proposes a test case generation technique that uses offloading as a generation parameter to overcome the lack of such techniques in previous studies. The proposed technique improves the coverage path on applications that use offloading, thereby improving the effectiveness and efficiency of penetration testing.

Keywords: Penetration testing · Software testing · Security testing
Test case generation

1 Introduction

Information technology security is a dominant issue. Most organisations are attempting to improve their security levels. To achieve this goal, firms attempt to uncover hidden security vulnerabilities in applications, networks and other devices that they use. Penetration testing can be used to discover such vulnerabilities. This practice was defined in a previous work as 'the art of finding an open door' [1]. Researchers are attempting to redefine and improve penetration testing by considering it a post-deployment vulnerability assessment task that is conducted as an isolated test process in a manual and even ad-hoc fashion [2–5].

P. Vasant et al. (Eds.): ICO 2018, AISC 866, pp. 267–276, 2019.
https://doi.org/10.1007/978-3-030-00979-3_27