Chapter 18
An Alternative Threat Model-Based Approach for Security Testing

Bouchaib Falah
Al Akhawayn University, Morocco

Mohammed Akour
Yarmouk University, Jordan

Samia Oukemeni
Al Akhawayn University, Morocco

ABSTRACT

In modern interaction, web applications has gained more and more popularity, which leads to a significate growth of exposure to malicious users and vulnerability attacks. This causes organizations and companies to lose valuable information and suffer from bad reputation. One of the effective mitigation practices is to perform security testing against the application before release it to the market. This solution won't protect web application 100% but it will test the application against malicious codes and reduce the high number of potential attacks on web application. One of known security testing approach is threat modeling, which provides an efficient technique to identify threats that can compromise system security. The authors proposed method, in this paper, focuses on improving the effectiveness of the categorization of threats by using Open 10 Web Application Security Project's (OWASP) that are the most critical web application security risks in generating threat trees in order to cover widely known security attacks.

1. INTRODUCTION

Software security testing has become a primary concern for software developers in order to preserve the confidentiality, integrity, availability, authorization, authentication and non-repudiation of their applications. Security testing is used to ensure the correctness of defensive mechanisms installed against attackers within the application. However, security testing is commonly misunderstood and treated as

DOI: 10.4018/978-1-5225-3422-8.ch018

an auxiliary concern in the lifecycle of software. According to National Vulnerability Database (NVD) (Florian, 2014), 13 new vulnerabilities per day were discovered in 2013, for a total of 4,794 security vulnerabilities a year and approximately one-third of these vulnerabilities were classified 'high severity'; in another word, an exploit of a vulnerability would have a high impact on the attacked assets and subsequently on the business processes.

Nowadays, web application vulnerabilities have become a major concern in software security because the popularity of web applications has increased and the nature of information streamlining through the internet such as financial transactions and credit card numbers has changed, as it becomes more sensitive and has a significant impact on the user privacy. Therefore, an effective security testing technique is needed to be integrated in testing process of software in order to protect the application form major attack patterns i.e. Cross Site Scripting (XSS), SQL injection, cross-site request forgery, JavaScript hijacking, and DNS rebinding. Although Software security testing field is quite new comparing to other types of software testing. Many researchers tried to develop different security testing methods and approaches that can be effective and efficient for building secure web applications and web services. One of these popular techniques is Threat Modeling (Marback, Do, He, Kondamarri & Xu, 2013). This technique uses threat trees to identify flaws and vulnerabilities in software and then generates test cases.

Marback et al. (Marback, Do, He, Kondamarri & Xu, 2013) proposed a threat model-based security testing approach that generates automatically test cases from threats trees categorized using STRIDE model (Swiderski, & Snyder, 2004). This model was developed by Microsoft by classifying threats according to the nature or the motivation of the threat. This model limits the proposed technique to a subset of possible threats. Hence, in our paper, we propose to expand the categorization model and address a large number of vulnerabilities through a comprehensive analysis of security vulnerabilities according to Open Web Application Security Project's (OWASP), 10 most critical Web application security risks.

This paper is organized as follows: Section 2 defines the threat model approach and discusses the background and limitation of the technique. Section 3 presents threat trees generated according to OWASP top 10. Section 4 concludes the paper and discusses future work.

2. THREAT MODELING

Threat modeling is the process of identifying, analyzing, and mitigating security threats for a system (Swiderski, & Snyder, 2004).. In another word, threat modeling can be similar to miss-use case diagram, where a set of action can be performed in the intention to damage the system (Michael & Steve, 2008; Microsoft, 2015). Threat modeling iteratively evaluates and ranks the potential threats and the proper techniques for reducing threats (Microsoft, 2015).

Threat modeling helps to model the interactions between the various components of an application, in order to (PasGates, 2010):

- Identify the information to protect;
- Define authorization and authentication issues;
- Define the external data input interfaces which will define the scope of tests to be performed;
- Define possible attacks;