Journal of Theoretical and Applied Information Technology
15th January 2022. Vol.100. No 1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

CATALOGUE-BASED GUIDELINE FOR MISUSE CASE

[1] MUHAMMAD ASYRAF KHAIRUDDIN, [2] ABDUL AZIM ABD GHANI, [2] HAZURA ZULZALIL, [2] SA'ADAH HASSAN

[1]Software Engineering Programme, Faculty of Computer Science & Information Technology, Universiti Malaysia Sarawak, Malaysia
[2]Software Engineering and Information System, Faculty of Computer Science & Information Technology, Universiti Putra Malaysia, Malaysia
E-mail: [1]kmasyraf@unimas.my, [2]{azim, hazura, saadah}@upm.edu.my

ABSTRACT

Misuse case is one of the security requirement elicitation techniques that are easy to use and learn. Unfortunately, the current guideline provided is too general. The process of identifying the misuse case and threats is open for the analyst's interpretation. Lack of knowledge in security threats also can make it worse. These problems can lead to analysis paralysis situation. In this paper, we proposed a catalogue-based guideline to support misuse case techniques to elicit security requirements. This guideline consists of two catalogues used to assist software developers in identifying attacks and threats from a misuse case diagram. We experimented with selected students to evaluate the effectiveness of the guideline in identifying threats and types of threats. We also evaluated the usability of the guideline by conducting experts reviews. Experiment's result shows sufficient evidence that using the misuse case with the proposed catalogue-based guideline is more effective in identifying threats and types of threats than using the misuse case without a guideline. Expert review's result also shows that the catalogue-based guideline is more usable in identifying threats than without using the guideline.

Keywords: *Misuse Case, Security Requirements, Threats, Catalogue, Guideline*

1. INTRODUCTION

One of the ways to elicit security requirements is by using the misuse case technique. Misuse case is easy to learn and understand by software developers as it is based on the commonly use Unified Modeling Language (UML) use case diagram. It can be considered as an extension to a use case diagram. By using a misuse case diagram, we only need to have several brainstorming sessions before we can identify threats or attacks that can happen to the system. However, there are several problems in which can hamper its performance to identify threats. The first problem is there are no exact guidelines provided to elicit security requirements. The instruction is too general and imprecise [1], where the process of identifying misuse cases and threats are open for the analyst' interpretation. This problem may lead to either the development of insecure software or analysis paralysis. Analysis paralysis often occurs due to overanalyzing or overthinking for a solution but end up with too many solutions and cannot decide which solution to take on. Thus, a proper guideline is needed to avoid analysis paralysis from happening.

The second problem is the knowledge gap in the security field. In order to identify the threats, the analyst needs to have particular knowledge of threats and attacks. That means the identifying process is depended on the analyst experience and knowledge. Most of the software developers do not have sufficient knowledge of security. Since more reliable and secure software is needed, software developers need to equip their development team with a security expert. However, getting the security expert to join the team may need extra cost for a smaller development team.

This paper aims to evaluate the catalogue-based guideline for misuse cases in identifying threats and types of threats and whether the proposed guideline is useful in identifying the threats.

2. RELATED WORKS

Several authors have proposed solutions and enhancements to improve the use of the misuse