A Unified Use-Misuse Case Model for Capturing and Analysing Safety and Security Requirements

O. T. Arogundade  
Chinese Academy of Sciences, China

A. T. Akinwale  
University of Agriculture, Abeokuta, Nigeria

Z. Jin  
Peking University, China

X. G. Yang  
Chinese Academy of Sciences, China

ABSTRACT

This paper proposes an enhanced use-misuse case model that allows both safety and security requirements to be captured during requirements elicitation. The proposed model extends the concept of misuse case by incorporating vulnerable use case and abuse case notations and relations that allows understanding and modeling different attackers and abusers behaviors during early stage of system development life cycle and finishes with a practical consistent combined model for engineering safety and security requirements.

The model was successfully applied using health care information system gathered through the university of Kansas HISPC project. The authors were able to capture both security and safety requirements necessary for effective functioning of the system. In order to enhance the integration of the proposed model into risk analysis, the authors give both textual and detailed description of the model. The authors compare the proposed approach with other existing methods that identify and analyze safety and security requirements and discovered that it captures more security and safety threats.

DOI: 10.4018/978-1-4666-2050-6.ch014
INTRODUCTION

Use case method is a research tool in Requirement Engineering (RE) field where the concept of use case is used to model functional requirements and misuse case is used to model non-functional requirements for a system. The use of use case is becoming popular for determining, communicating, specifying and documenting requirements (Constantine & Lockwood, 1999; Cockburn, 2001; Jacobson et al., 1992; Kulak & Guiney, 2000; Rumbaugh, 1994). Misuse case, the extension of use case by Sindre and Opdahl (2005), allows the concept of use case to be useful in eliciting non-functional requirements. Safety and security requirements are often developed independently of the rest of the requirements engineering activity and hence are not integrated into the mainstream of the requirements activities. As a result, safety and security requirements that are specific to the system and that provide for protection of essential services, features and assets are often neglected (Mead, 2007).

The ad hoc integration of safety and security mechanisms into a software system which has already been developed has a negative impact on the maintainability and security of the system (Eduardo, Jurjens, Trujillo, & Sushil, 2009).

With the ever increasing exploitation of networking technologies, it is now imperative that both safety and security will be taken into account during the early stage of system development life cycle (Harrison & Sujan, 2008).

In our initial work (Arogundade et al., in press) we have introduced vulnerable use case including inside abuser in order to address the issue of deliberate act for safety concerns. This paper refines this initial work by proposing an enhanced use-misuse case model for eliciting and analyzing safety and security requirements in a unified framework. The ideas in this paper have been applied to one realistic case study, the e-health care system. The e-health care information used in this paper is retrieved from Health Information Technology Resource Toolkit developed through the university of Kansas HISPC project (http://ehealth.kansashealthonline.org).

Safety vs. Security

In some stream of research the differences they claim between safety and security are often very narrow to be comprehended. Some authors, e.g., Firesmith (2003), use the term security for what concerns malicious (or deliberate) harm on the IS, and they use the term safety for what concerns accidental harm on the IS. This author used the broader notion of survivability to cover both security (in the above sense) and safety. The same notion was adopted by Sindre (2007). The notion of security and safety that we adopt in this work, and that defines our scope, is broader. We are looking at both deliberate and accidental safety and security incidents distinctly. We therefore refer to both safety and security as safeguard (Figure 1).

We define safety as ‘avoidance of accidents and mishaps (unplanned events) that result in death, injury, illness, damage to or loss of property or environmental harm’. These unplanned events are caused by either planned actions (deliberate) or unplanned actions. The unplanned actions are the accidental incidents (mistakes or faults) while the planned actions are the deliberate incidents. In IS safety the purpose of deliberate incidents is not directly related to the incident and consequences. The deliberate incident within IS safety do not want incidents to happen, the deliberate acts are made in order to do work more efficiently and less effortful (the abuse case in the use-misuse case model). The deliberate acts can be characterized as cynical, calculating and ignorant. The intention behind both the planned and unplanned actions in IS safety is not malicious but the consequences can be grave.

We defined security as ‘protection against planned and unplanned events in order to attain fundamental objectives of preserving the confidentiality, integrity and availability of informa-