Supporting Consistency
during the Development and
Evolution of Quality Unified
Use-Misuse Case Models

Mohamed El-Attar, Department of Computer Science and Engineering, Mississippi State
University, Starkville, MS, USA

ABSTRACT

In the domain of scenario-based modeling, use case modeling has been extended several times to introduce security related concepts such as misuse, abuse, vulnerability and safeguarding. The most advanced model is the Unified Use-Misuse Case Model (UUMCM) (Arogundade et. al., 2011). A low quality UUMCM will not only cause the development of a system that does not meet its business requirements, but also a system that is insecure. This paper proposes an authoring structure that specifically designed to improve one particular quality attribute; structural consistency. Automation support has been developed for this structure. Two different approaches have been used to demonstrate the feasibility and application of the proposed structure. In both validation approaches, the results show that the structure can be used to ensure structural consistency in UUMCMs throughout their development and evolution.

Keywords: Abuse Cases, Misuse Cases, Mitigates, Structural Consistency, Threatens, Use Cases

1. INTRODUCTION

Nowadays security is indispensable quality attribute for many systems. There is a constant threat of a multitude of attacks that can risk the integrity of a system. Systems must be able to perform and deliver their business values securely even when attacked otherwise they will be deemed untrustworthy. Conventional software engineering processes focuses on the development of system functionality that realizes business needs while security being considered after functionality development is completed; an afterthought. Systems are then patched with defensive mechanisms such as cryptographic components, IDS (Intrusion Detection System) and firewalls. Such approaches to security are insufficient and likely lead to costly reworks (Jürjens, 2004). Instead, software systems should be development using a secure software engineering process. Secure software engineering states that security concerns should be taken into account as early as possible in the development life cycle (Dubois & Wu, 1996; Mead, 2007).

DOI: 10.4018/IJSSE.2015100101
Use case modeling is a very popular requirements engineering technique for eliciting, specifying and communicating functional requirements of a system (OMG, 2003). Use case modeling has a relatively simple syntax which enables non-technical stakeholders to comprehend and provide vital feedback. Another key reason for the success and popularity of use case modeling is its scenario-based approach to specifying requirements. Scenario-based specifications are widely accepted in requirements engineering as it offers a natural way to describe the behavior of systems, which in many cases occur as usage examples. It has been shown through an industrial survey that scenarios are an effective technique to determine and validate requirements (Weidenhaupt et al., 1998). Several research works have devised approaches to secure software development by leveraging the popularity of use case modeling, most notably misuse cases (Sindre & Opdahl, 2005) and abuse cases (McDermott & Fox, 1999). Misuse and abuse cases were both introduced as extensions to use case modeling. The behavioral machination and notation of misuse and abuse cases are similar to use cases, however they are semantically the inverse of use cases. Although misuse and abuse cases are ostensibly equivalent, there are distinct contrasts between them which have been outlined in great detail in Chun Wei (2005). In Chun Wei (2005), differences between misuse and abuse case modeling with respect to concept and intent; content and level of detail; notation; and how they are developed, have been presented. The contrasts between misuse and abuse cases lead to the conclusion that they are both useful use case-based tools for functional security modeling of which neither can substitute for the other. In fact, the Unified Use-Misuse Case Model (UUMCM) has been proposed by Arogundade et al. (2011) to satisfy the need to include both misuse and abuse cases within the same model. The UUMCM will be the focal model of this paper as we consider it to be the most advanced use case-based security modeling technique to date. A use case model consists of a diagram depicting use cases, actors and relationships between them, and it consists of textual descriptions explaining the use cases and actors. Similarly, the UUMCM consists of a diagram containing use, misuse and abuse cases, actors, misusers and abusers, and relationships between them. The UUMCM also consists of textual descriptions explaining the use, misuse and abuse cases, and actors, misusers and abusers.

A number of templates have been proposed to describe misuse cases (Sindre & Opdahl, 2001). Many of the templates are based on embedding the description of misuse behavior within already-popular use case templates, such as those presented in Cockburn (1997, 2001), Constantine (1995), Kruchten (1999). Other more “extensive” templates have been proposed by Sindre & Opdahl (2001, 2005) that are solely dedicated to narrating misuse cases only. Authoring abuse cases requires a detailed description of their actors’ resources, skills and objectives (Chun Wei, 2005). All the proposed templates and methods that can be used to describe misuse and abuse cases prescribe the use of syntax-free natural language. Syntax-free natural language is attractive due to its expressiveness and understandability, particularly with non-technical stakeholders. However, syntax-free natural language is inherently ambiguous thus hampering several quality attributes desired in a use case-based security model, particularly for this paper, the UUMCM. A number of use case modeling quality attributes have been proposed in the literature. A comprehensive compilation and categorization of quality attributes for use case models have been presented in El-Attar & Miller (2012). The compilation of quality attributes for use case models proposed in El-Attar & Miller (2012) was developed via a systematic literature review. According to in El-Attar & Miller (2012), quality in use case models are categorized into five main categories: consistency, correctness, completeness, analytical value and understandability. Given the similarity and behavioral machination between use, misuse and abuse cases, it can be inferred that the quality attributes for use case models as proposed in in El-Attar & Miller (2012) are also applicable to the UUMCM. Many research works have been devoted to improve various quality attributes in use case models. In this paper, the focal quality attribute is consistency.
Modeling a Simple Self-Organizing System
www.igi-global.com/chapter/modeling-a-simple-self-organizing-system/108813?camid=4v1a

From Frequent Features to Frequent Social Links
www.igi-global.com/article/from-frequent-features-to-frequent-social-links/80197?camid=4v1a

Using Goal Models Downstream: A Systematic Roadmap and Literature Review
www.igi-global.com/article/using-goal-models-downstream/126305?camid=4v1a