Improving Security and Safety Modelling with Failure Sequence Diagrams

Andreas Opdahl, University of Bergen, Norway

Christian Raspotnig, University of Bergen, Norway

ABSTRACT

While security assessments of information systems are being increasingly performed with support of security modelling, safety assessments are still undertaken with traditional techniques such as Failure Mode and Effect Analysis (FMEA). As system modelling is becoming an increasingly important part of developing more safety critical systems, the safety field can benefit from security techniques that integrate system modelling and security aspects. This paper adapts an existing security modelling technique, Misuse Sequence Diagrams, to support failure analysis. The resulting technique, called Failure Sequence Diagrams, is used to support Failure Mode and Effect Analysis in an industrial setting. Based on the experiences, the authors suggest improvements both to traditional safety techniques and to security and safety modelling.

Keywords: *Case Study, Failure Mode and Effect Analysis, Failure Sequence Diagrams, Field Experiment, Information Systems, Misuse Sequence Diagrams, Safety, Security Modelling, Sequence Diagrams*

1. INTRODUCTION

Modelling has become an integral part of developing information systems, and modelling languages such as UML (OMG, 2011) are widely used in many domains today (Watson, 2011). One of the reasons for UML's popularity is that it uses visualization to ease communication between stakeholders with various backgrounds (Watson, 2011). This has also been recognized in the security field (Sindre & Opdahl, 2005), and techniques combining UML and security aspects have become popular for developing information systems. The safety field continues to rely on traditional techniques, such as Hazard and Operability studies (HAZOP) and Failure Mode and Effect Analysis (FMEA) (Ericson, 2005). Even though these techniques can be used along with system models, they do not offer a way to integrate safety aspects into the models to support visualization during the safety assessments that involve communication between different stakeholders. What they do offer during the safety assessments, on the other hand, is a structured process for communicating and collecting information, which some security modelling techniques

DOI: 10.4018/jsse.2012010102

lack. Common to the security and safety fields is that important security and safety aspects must be communicated amongst stakeholders during the information systems development. If communication fails, it can lead to fatal mishaps and to useless systems.

We have therefore investigated how to use a security modelling technique in combination with a traditional safety technique in an industrial setting. For security modelling technique, we propose Failure Sequence Diagrams (FSD), which adapts Misuse sequence diagrams (MUSD) to failure analysis. We chose MUSD as our starting point because it has been shown to be well suited for visualizing interactions between system components during an intrusion (Katta, Karpati, Opdahl, Raspotnig, & Sindre, 2010). For traditional safety technique, we use FMEA, which systematically addresses failure modes of components and investigates how they affect the system (Ericson, 2005). Our primary aim was to investigate whether FMEA could benefit from being combined with FSD for visualizing component interaction. We also wanted to investigate whether this could somehow improve security modelling with MUSD and to gain experiences from industrial use of FSD. Our research is part of a larger project, *ReqSec – Requirements Engineering for Security*, that investigates more broadly how modelling notations can be used to involve stakeholders in security requirements work (ReqSec project, 2008).

To investigate how FSD can be used to support FMEA, we have conducted an empirical study in the Air Traffic Management (ATM) domain using research methods from case studies and field experiments. Our study shows that FSD can be used to support FMEA in at least three different ways: either using FMEA first before applying FSD to the results; using FSD first before summarize the results with FMEA; or, most beneficially in our case, using FSD and FMEA in parallel in an iterative way. Experiences with the three strategies are reported and discussed with an eye to how FSD (and thus MUSD) can be improved in further work. For example, even though we consider our proposed new way of modelling security and safety with sequence diagrams to be viable, we recognize that it needs further improvements, in particular for handling complexity. We also compare the safety and security fields more broadly, looking at how MUSD and FSD can be combined with other techniques, both traditional safety techniques and security modelling techniques.

The paper is structured as follows. Section 2 describes the background for the research along with relevant work. Section 3 describes the research method used for obtaining the results that are presented in Section 4 and discussed further in Section 5. Finally, Section 6 concludes the paper and looks ahead at further work.

2. BACKGROUND

A system failure is defined as "an event that occurs when the delivered service deviates from the correct service" (Avizienis, Laprie, & Randell, 2001). The relationship between fault, error and failure is further described with respect to dependability, together with how it relates to interacting system components and how it is relevant both to safety and security aspects (Avizienis et al., 2001).

Failure Mode and Effect Analysis (FMEA) is not only used for identifying the failure modes of system components and their effects, but also for finding the causal factors causing the failure to occur. This is typically done by using a worksheet, and it follows the idea with respect to faults, errors and failures. Although FMEA relates failure modes to system components and to the complete system, it does not address interactions between components in particular. FMEA was originally used for reliability analysis and is now commonly used in safety assessments (Ericson, 2005), but it has also been applied in security assessments (Aagedal et al., 2002).

Misuse Sequence Diagrams (MUSD) is a system security technique that we have developed previously to give an overview of an attack sequence during an intrusion (Katta et al., 2010). It refines the misuse case (MUC)