Chapter 85
Threat Analysis in Goal-Oriented Security Requirements Modelling

Per Håkon Meland
SINTEF ICT, Norway

Elda Paja
University of Trento, Italy

Erlend Andreas Gjære
SINTEF ICT, Norway

Stéphane Paul
Critical Embedded Systems Laboratory, Thales Research and Technology, France

Fabiano Dalpiaz
Buys Ballot Laboratory, Utrecht University, The Netherlands

Paolo Giorgini
University of Trento, Italy

ABSTRACT

Goal and threat modelling are important activities of security requirements engineering: goals express why a system is needed, while threats motivate the need for security. Unfortunately, existing approaches mostly consider goals and threats separately, and thus neglect the mutual influence between them. In this paper, the authors address this deficiency by proposing an approach that extends goal modelling with threat modelling and analysis. The authors show that this effort is not trivial and a trade-off between visual expressiveness, usability and usefulness has to be considered. Specifically, the authors integrate threat modelling with the socio-technical security modelling language (STS-ml), introduce automated analysis techniques that propagate threats in the combined models, and present tool support that enables reuse of threats facilitated by a threat repository. The authors illustrate their approach on a case study

DOI: 10.4018/978-1-5225-3923-0.ch085

from the Air Traffic Management (ATM) domain, from which they extract some practical challenges. The authors conclude that threats provide a useful foundation and justification for the security requirements that the authors derive from goal modelling, but this should not be considered as a replacement to risk assessment. The usage of goals and threats early in the development process allows raising awareness of high-level security issues that occur regardless of the chosen technology and organizational processes.

1. INTRODUCTION

Modern systems are becoming more and more complex and dynamic, as they involve a multitude of autonomous subsystems and human actors that interact in unpredictable manners (Sommerville et al., 2012). These large and complex systems are highly exposed to malicious intents, and they need to exhibit adaptive behaviour at runtime to continue delivering their purpose without failing (Dalpiaz, Giorgini, & Mylopoulos, 2013).

As in any engineering discipline, early awareness and analysis of potential problems is beneficial to system design, enabling the development of more robust systems. We investigate the usage of threat modelling and analysis in goal-oriented security requirements engineering. This helps not only the elicitation of security requirements, but also the definition of adaptation triggers, i.e., the circumstances under which a system shall adapt.

Threat modelling is typically regarded as the analysis of how a system can be exploited in malicious ways. However, as there is no well-accepted standard for conducting threat modelling, the chosen technique is subject to trade-offs that take into account the analysis' purpose (Meland & Gjære, 2012). Threat modelling can, for instance, be asset-centric, attacker-centric, or software-centric (Shostack, 2008). Though a number of somewhat overlapping threat modelling techniques and approaches exist, there is general consensus that (i) threat awareness is of great benefit for performing risk assessment and for eliciting security requirements in the early phases of the software development lifecycle, and (ii) threat modelling and analysis should be repeated as more information about the system becomes available.

Goal modelling is the a state-of-the-art technique in requirements engineering (E. Yu & Mylopoulos, 1998) to understand *why* a certain requirement exists and how it is related to the goals and needs of stakeholders. Moreover, goal modelling comes with refinement mechanisms that support the clarification process, and offers techniques to identify conflicts early in the system development.

Goal models have been extensively used in security requirements too (Giorgini, Massacci, Mylopoulos, & Zannone, 2005; Mouratidis & Giorgini, 2007; Liu, Yu, & Mylopoulos, 2003; Lamsweerde, 2004). However, their combined usage with threats has not been adequately investigated yet and typically goal modelling and threat modelling are conducted as independent activities.

The research question we address in this paper is "*to what extent should we include threats in goal-oriented modelling?*" We believe there is no straightforward answer to this question, and we argue that risk assessment shall be conducted as a separated activity, and not as part of goal modelling (as, for instance, in Asnar, Giorgini, and Mylopoulos (2011)), for different reasons. Firstly, when adding additional concepts to a modelling language, we need to consider the impact on its complexity and usability (Moody, 2009). For instance, Moody defines *visual expressiveness* to be the number of visual variables used in a notation. Having a rich vocabulary is of great value when you want to describe necessary details, improving usefulness, but requires more effort to learn; hence it could also affect usability. Sec-