Data & Knowledge Engineering 68 (2009) 579–598

Contents lists available at ScienceDirect

Data & Knowledge Engineering

journal homepage: www.elsevier.com/locate/datak

Modeling and analysis of security trade-offs – A goal oriented approach

Golnaz Elahi [a,*], Eric Yu [b]

[a] Department of Computer Science, University of Toronto, Canada M5S 1A4
[b] Faculty of Information, University of Toronto, Canada M5S 3G6

ARTICLE INFO

Article history:
Available online 27 February 2009

Keywords:
Security trade-offs
Trade-off analysis
Conceptual modeling
Goal modeling
Goal model evaluation

ABSTRACT

In designing software systems, security is typically only one design objective among many. It may compete with other objectives such as functionality, usability, and performance. Too often, security mechanisms such as firewalls, access control, or encryption are adopted without explicit recognition of competing design objectives and their origins in stakeholders' interests. Recently, there is increasing acknowledgement that security is ultimately about trade-offs. One can only aim for "good enough" security, given the competing demands from many parties. This paper investigates the criteria for a conceptual modeling technique for making security trade-offs. We examine how conceptual modeling can provide explicit and systematic support for modeling and analyzing security trade-offs. We examine several existing approaches for dealing with trade-offs and security trade-offs in particular. From analyzing the limitations of existing methods, we propose an extension to the i* Framework for security trade-off analysis, taking advantage of its multi-agent and goal orientation. The method was applied to several case studies used to exemplify existing approaches. The resulting models developed using different approaches are compared.

1. Introduction

"Security is about trade-offs, not absolutes."
Ravi Sandhu

In designing software systems, security is typically only one design objective among many. Security safeguards may conflict with usability, performance, and even functionality. For example, if usability concerns are not addressed in the design of a secure system, users respond by circumventing security mechanisms [1,2]. Achieving a balance between the intrusiveness of security mechanisms [3] and usability goals is an important consideration in designing successful secure software systems. Security goals can have their own contradictions because confidentiality, integrity, privacy, accountability, availability, and recovery from security attacks often conflict fundamentally. For example, accountability requires a strong audit trail and end-user authentication, which conflicts with privacy needs for user anonymity [3].

Ultimately, security is about balancing the trade-offs among the competing goals of multiple actors to achieve a "good enough" security. In current practice, security designers often adopt security mechanisms such as firewalls, access control, or encryption without explicit recognition of, and systematic treatment of competing design objectives originating from various stakeholders. While risk assessment methods such as [4,5] address balancing the costs and effects of security solutions to achieve good enough security, assuming security costs and benefits are measurable, this paper focuses on qualitatively analyzing trade-offs that security goals and alternative security solutions impose on other quality objectives.

* Corresponding author.
E-mail addresses: gelahi@cs.toronto.edu (G. Elahi), eric.yu@utoronto.ca (E. Yu).

0169-023X/$ - see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.datak.2009.02.004

This question then arises: what conceptual modeling techniques can be used to help designers analyze security trade-offs to achieve "good enough" security? To our knowledge, existing conceptual modeling techniques for modeling security-related information and trade-off analysis techniques do not raise and answer this question.

The remaining parts of this paper are structured as follows. In Section 2, we consider the criteria for a suitable conceptual modeling technique for dealing with security trade-offs. In Section 3, a number of existing approaches to security trade-off analysis are reviewed and compared to the introduced criteria. From analyzing the limitations of existing methods, in Section 4, we propose a conceptual modeling technique for modeling and analyzing security trade-offs in a multi-actor setting. The meta-model of security concepts is introduced as well. In Section 5, we describe the goal model evaluation and trade-off analysis technique. Section 6 summarizes the results of some case studies. Finally, Section 7 discusses the results and limitations of the approach.

2. Conceptual modeling criteria for security trade-offs analysis

Trade-off analysis is a systematic examination of the advantages and disadvantages of requirements and/or design choices for a system to achieve the right balance among several competing goals [6]. When some goals are not sufficiently satisfied, designers need to explore further alternatives that can better achieve those goals, without detrimentally hurting the others. Each potential solution can have positive effects on the achievements of some goals while having negative effects on others. A careful and systematic process for security trade-off analysis can be very challenging, because to resolve security trade-offs one need to consider competing goals of multiple stakeholders, risk of attacks, security countermeasure, and their impacts.

In this context, we ask: what are the criteria for a proper conceptual modeling technique for dealing with security trade-offs? What concepts need to be modeled, and how are they involved in the trade-off analysis? In many engineering disciplines, trade-offs are analyzed using detailed mathematical models. However, in designing secure software systems, multiple stakeholders with diverse, incommensurable, and competing goals impose security trade-offs that cannot be reduced easily to mathematical functions. Conceptual modeling techniques, on the other hand, offer the possibility of analyzing the factors that contribute to trade-offs and their structural compositions and relationships.

The conceptual foundation for trade-off modeling needs to convey the idea that attempting to improve one quality can adversely affect other quality objectives. Therefore, the conceptual modeling technique needs to provide conceptual constructs to express: (1) design goals and objectives, alternative operationalizations to achieve the objectives, and the impacts of alternative operationalizations on goals and solutions; (2) actors who seek alternative design solutions to achieve their individual goals and objectives. Furthermore, security objectives are not affected only by alternative security solutions and operationalizations of quality goals. In case of security goals, the trade-off constructs need to express; (3) threat of external/internal actors and vulnerabilities that impact security and other requirements.

Design goals and objectives

Security and other trade-offs take root from conflicts among design objectives that originate from stakeholder goals. While selecting a security solution among alternatives is difficult, the more fundamental problem is that designers need to decide about alternate security mechanisms subject to multiple factors such as cost, time-to-market, various non-functional requirements (NFRs), security policies, standards, and individual goals of various stakeholders. Therefore, the conceptual foundation for expressing trade-offs needs to provide means for modeling stakeholders' goals and design objectives. By modeling the alternative solutions that operationalize the objectives and structuring the impact of operationalizations on the goals, one can analyze what causes trade-offs among objectives. To resolve the trade-offs, the model needs to express the extents to which design objectives are satisfied or denied. The extents or measures could be quantitative or qualitative. Quantitative approaches can greatly simplify decision making, but can be difficult to apply due to lack of agreed metrics, subjective quality requirements, or unavailability of accurate measures in the early stages of the system development. The modeling technique should be able to support analysis despite inaccurate, incomplete, or subjective knowledge about goals as well.

Actors

Design objectives typically originate from multiple sources and stakeholders such as the system's users, administrators, top managers, project managers, and customers. The conceptual modeling technique needs to consider multiple actors that impose competing goals on the designer. The modeling technique should be able to model trade-offs that occur within a single actor or across multiple actors.

Security-specific concepts

Security requirements are needed because of the threat of malicious actors. Achievement of security objectives are affected by threats of internal or external actors and existence of vulnerabilities in system design. Trade-offs cannot be resolved without relating the impacts of attacks and exploitation of vulnerabilities on the systems functionality and quality objectives. Therefore, the conceptual modeling technique for modeling security trade-off needs to model security-specific