Chapter II

Arguing Satisfaction of Security Requirements

C. B. Haley, The Open University, UK
R. Laney, The Open University, UK
J. D. Moffett, The Open University, UK
B. Nuseibeh, The Open University, UK

ABSTRACT

This chapter presents a process for security requirements elicitation and analysis, based around the construction of a satisfaction argument for the security of a system. The process starts with the enumeration of security goals based on assets in the system, then uses these goals to derive security requirements in the form of constraints. Next, a satisfaction argument for the system is constructed, using a problem-centered representation, a formal proof to analyze properties that can be demonstrated, and structured informal argumentation of the assumptions exposed during construction of the argument. Constructing the satisfaction argument can expose missing and inconsistent assumptions about system context and behavior that effect security, and a completed argument provides assurances that a system can respect its security requirements.
INTRODUCTION

This chapter describes an approach to carry out security requirements engineering; the process of eliciting, specifying, and analyzing the security requirements for a system. The approach is founded on the following fundamental ideas:

- The “what” of security requirements — its core artifacts — must be understood before the “how” of their construction and analysis.
- Security cannot be considered as a feature of software alone; it is concerned with the prevention of harm in the real world. We must therefore consider both the security requirements of real-world systems and the specification of software that demonstrably meets those requirements.
- Since security is largely concerned with prevention of misuse of system functions, security requirements can most usefully be defined by considering them as constraints upon functional requirements.
- Since security is by definition an “open world” problem (the domain of analysis will always be too small), any argument that a system will satisfy its security requirements must take non-provable assertions about the real world into account.

The contribution of this chapter is the combination of four components described in previous work into a coherent security requirements process. The first component is a framework that provides a systematic statement of the roles and relationships of security goals, security requirements, and security functions, and their relationships with other system and software requirements. The second is a way of describing threats and their interactions with the system. The third is a precise definition of security requirements. The fourth is a two-layer set of arguments to assist with validating the security requirements within the context of the system, to determine that the system is able to meet the security requirements placed upon it. The first and third were described in Moffett, Haley, and Nuseibeh (2004), the second in Haley, Laney, and Nuseibeh (2004), and the fourth in Haley, Moffett, Laney, and Nuseibeh (2005).

Although all the steps in the process are described in this chapter, the third component — argumentation — is emphasized. This is not an exclusive focus, though, as understanding the role of argumentation in security requirements requires that one understand the first three parts of the process in order to place the pieces correctly in context.

The next section discusses the security requirements process, while the following section provides information about argumentation driven problem analysis. The two subsequent sections present the major steps of the process and illustrate it with the aid of a case study. The following section discusses the proposed approach and the section after introduces related work. The final section concludes the chapter.