Revisiting Architectural Tactics for Security

Eduardo B. Fernandez[1(✉)], Hernán Astudillo[2], and Gilberto Pedraza-García[3,4]

[1] Florida Atlantic University, Boca Raton, FL, USA
ed@cse.fau.edu
[2] Departamento de Informática, Universidad Técnica Federico Santa María, Valparaíso, Chile
hernan@inf.utfsm.cl
[3] Universidad de Los Andes, Bogotá, Colombia
g.pedraza56@uniandes.edu.co
[4] Programa de Ingeniería de Sistemas, Universidad Piloto de Colombia, Bogotá, Colombia

Abstract. Architectural tactics are design decisions intended to improve some system quality factor. Since their initial formulation, they have been formalized, compared with patterns and associated to styles, but the initial set of tactics for security has only been refined once. We have examined this tactics set and classification from the viewpoint of security research, and concluded that some tactics would be better described as principles or policies, some are not needed, and others do not cover the functions needed to secure systems, which makes them not very useful for designers. We propose here a refined set and classification of architectural tactics for security, which we consider more appropriate than the original and the previously refined sets. We also suggest how to realize them using security patterns.

Keywords: Architecture tactics · Secure architectures · Security patterns · Secure software development

1 Introduction

Secure systems are notoriously hard to build; like most global system quality criteria, a piecemeal approach based on securing system elements is simply inappropriate. Design decisions have a global effect on other quality attributes, e.g. availability, and thus local optimizations are not possible. From a security research standpoint, lacking quantitative measures, a secure system is one that can be shown to withstand a variety of attacks; although many approaches to build secure systems have been proposed [25], they usually focus on some specific aspect, e.g. authorization, and address only one type of threat.

The security research literature describes many ways to secure specific parts of a system, to build secure systems, or to stop specific attacks, but few studies exist about how to make a whole system secure [8, 17, 25, 30]. On the other hand, the software architecture literature addressed security as one of several global quality properties, and proposes using "architectural tactics" [2, 3]; however, the specific proposed tactics are not justified on coverage or parsimony grounds, thus largely ignoring the existing research work on security. Also, security tactics give general guidance but

D. Weyns et al. (Eds.): ECSA 2015, LNCS 9278, pp. 55–69, 2015.
DOI: 10.1007/978-3-319-23727-5_5

not detailed construction advice; in fact, tactics are not mentioned in any of the best-known secure development methodologies [25].

Since their initial formulation, tactics have been formalized [1], compared with patterns [19], associated to the Common Criteria [18], and associated to styles [15]. However, the initial set of tactics for security [2, 3] has been refined only once [21]. This article presents a reasoned examination, pruning and reclassification of architectural tactics for security, considering both the original set and the refined set and applying security knowledge. We also consider a possible realization using security patterns; tactics require a convenient realization to provide detailed guidance to architects. *Patterns* are encapsulated solutions to recurrent problems in specific contexts, *security patterns* define solutions to handle threats or to fix a vulnerability [10]. Patterns are considered a good way to build secure systems and several methodologies based on them exist [7, 10, 25]. Patterns include several sections that define in addition to a solution, their use, applicability, advantages, and disadvantages. Other software architecture quality factors such as reliability, availability, and safety are also important, but we concentrate on security in this paper.

This article contributions include:

- A discussion of the correspondence of some security and software architecture concepts to understand them better. The security and software architecture communities are rather disjoint and we attempt to help bridge their gap.
- A revised set of tactics, based on security knowledge, which is our main contribution
- A detailed consideration of the use of security patterns as a way for realizing tactics.

The remainder of the article is organized as follows: Section 2 describes architecture tactics; Section 3 discusses security patterns; Section 4 defines security principles and policies, and other terms used for secure systems design; Section 5 examines the initial (and still used) tactics tree and indicates its problems; Section 6 presents some new tactics based on security knowledge; Section 7 proposes a realization for tactics using security patterns; Section 8 discusses related work; and Section 9 summarizes and concludes.

2 Architectural Tactics to Build Secure Systems

Architectural tactics, originally introduced in 2003 [2], are “measures” or “decisions” taken to improve some quality factor, a definition later refined to “architectural building blocks from which architectural patterns are created” [3]. Each tactic corresponds to a design decision with respect to a quality factor; i.e., tactics codify and record best practices for achieving that factor.

Rozanski and Woods [30, 31] defined architectural tactics as architectural design guidance, i.e. strategies or advice on how to drive a general design issue related to improving required quality attributes without imposing a particular software structure. They also suggest (but give little operational detail) that the application of security tactics may be expressed in the software architecture as adding, modifying, or deleting architectural elements with specific responsibilities, introducing security technologies, or describing new operational procedures to support secure operation.