Chapter 29
Agile Development of Security-Critical Enterprise System

Xiaocheng Ge
University of York, UK

ABSTRACT

The effective provision of security in an agile development requires a new approach: traditional security practices are bound to equally traditional development methods. However, there are concerns that security is difficult to build incrementally, and can prove prohibitively expensive to refactor. This chapter describes how to grow security, organically, within an agile project, by using an incremental security architecture that evolves with the code. The architecture provides an essential bridge between system-wide security properties and implementation mechanisms, a focus for understanding security in the project, and a trigger for security refactoring. The chapter also describes criteria that allow implementers to recognize when refactoring is needed, and a concrete example that contrasts incremental and "top-down" architectures.

INTRODUCTION

An enterprise system is an information system that promises a seamless integration of all the applications that process the information in an organisation. It provides a technical platform that enables organisations to integrate and coordinate their business processes. The concept and adaption of enterprise systems have attracted increasing interests as organisations have been seeking how they do their business more efficiently. However, if an organisation rushes to install an enterprise system without first having a clearing understanding of the business implications, the dream of integration can quickly turn into a nightmare. To avoid the problems, it is necessary to have a good understanding of aspects related to the applications, including the business characteristics; processes and architecture of the applications. Service oriented architecture (SOA) is an architectural style promoting the concept of business-aligned enterprise service as the fundamental unit of designing, building, and composing enterprise business solutions. The primary goal of SOA is to align the business world with the world of information technology (IT) in a way that makes both more effective. SOA is a bridge that creates a symbiotic and synergistic relationship between

DOI: 10.4018/978-1-4666-8111-8.ch029

the two that is more powerful and valuable than anything that we've experienced in the past. Moreover, SOA is about the business results that can be achieved from having better alignment between the business and IT. It represents a set of architectural principles that position software services as the primary means through which business services are offered by the organisation to its ecosystem. SOA is also becoming an important concept in the development of software applications. It provides a systematic solution to transform the development of a software application from a heavyweight process to an iterative and incremental one.

Securing access to information is important to any business. For a long time, security has been one of the major concerns in the development and the operation of all types of information systems (Amoroso 1994; Anderson 2001; Pfleeger and Pfleeger 2003; McGraw 2006). Security is a system issue that takes into account both security mechanisms (such as access control) and the engineering of security (such as a robust design that makes it difficult for software attacks to succeed). Sometimes these overlap, but often they do not. Security engineering is concerned with building secure system, and it has a layered architecture (Ge 2007). On the top of this architecture, it is the application security. The focus of this monograph is application security, which can be seen as a software engineering problem where the system is designed to resist attacks. The engineering of application security relies heavily on the discipline of software engineering, liberally borrowing methods that work and making use of critical engineering artefacts. A sound software engineering method is a prerequisite to sound software security. After decades of efforts, it is well accepted that security considerations should be taken into account at every stage of the application (system) development life cycle (Eric A. Fisch 2000; Anderson 2001; Viega and McGraw 2002; Grance, Hash et al. 2003; Pfleeger and Pfleeger 2003; Apvrille and Pourzandi 2005; McGraw 2006).

Security becomes even more critical for implementations structured according to service-oriented architecture (SOA) principles, due to loose coupling of services and applications, and moreover their possible operations across trust boundaries. On the other hand, to enable a business so that its processes and applications are flexible, changes to both process and application logic, as well as to the policies associated with them, including security access policies, are expected. The topic on this chapter is an agile development/integration of a secure enterprise system which has a service-oriented architecture. It covers three fields: enterprise system security, agile development, and SOA. In this chapter, we will focus on the relationship of these three elements from the perspective of security engineering, since the discussions from different angles are covered in other chapters in this book.

The rest of this paper is divided into two main parts. The first part provides a criterion for architectural security: what constitutes an iterative architecture, what properties it should uphold, and how it fits into an agile development process. The second part of the paper gives a concrete example, drawn from the practical work that motivated this approach.

BACKGROUND

In recent years, the principles and practices of agile software development have aroused enormous interests. The driver of developing software systems using agile software methods is to better manage different kinds of change. Agile development naturally matches stakeholders' needs for incremental delivery, and is therefore becoming the method of choice; however, little has been done to understand how security can be fully integrated in an incremental development. Several researchers have contrasted Agile or XP developments with traditional security engineering processes (Baskerville 1993; Abrahamsson, Warsta et al.