Chapter 46
Assessing the Security of Software Configurations

Afonso Araújo Neto
University of Coimbra, Portugal

Marco Vieira
University of Coimbra, Portugal

ABSTRACT

Security evaluation is a complex problem. As more and more software systems become available, more diversity and alternatives can be found to accomplish the same tasks. However, there is still a lack of a standard approach that can be used to choose among the available alternatives or evaluate their configuration security. In this chapter, the authors present a methodology to devise security appraisals, which is based on the collection of widespread security knowledge for a specific domain. They demonstrate their methodology by devising two specific appraisals for the domain of transactional systems. The first one can be used to evaluate and assess the configuration of an already deployed database installation, while the target of the second one is to compare the capability of specific database brands concerning security aspects. The authors also present a real demonstration of both appraisals in real scenarios.

INTRODUCTION

In most software systems, security is dependent not only on the inexistence of software vulnerabilities, but also on the actual software capabilities and the configuration used. Configuring a system for high security is frequently addressed in an intuitive manner and its success depends on several aspects that, by definition, cannot be known in advance: Who are the attackers? What tools and knowledge do they have? What are their goals? These questions raise a major issue: what should the user look for in a given software in terms of security mechanisms?

When dealing with very complex software, like, for instance, a database management system (DBMS), selecting the best alternative and finding the best configuration are difficult and highly time consuming tasks. This often leads to security vulnerabilities due to the use of inappropriate soft-

DOI: 10.4018/978-1-4666-4301-7.ch046

ware or due to configuration problems (Bellovin & Bush, 2009). This way, we urge the definition of tools to assess and compare the security of software configurations and products.

Several security evaluation methods have been proposed in the past (Bertino et al., 1995; Castano et al., 1994; Department of Defense, 1985; Pernul & Luef, 1992; Schell & Heckman, 1987). However, to the best of our knowledge, none of the existing methods is oriented towards the comparison of software products or configuration alternatives. Furthermore, practical experience shows that these methods are very complex and cannot be easily used by system administrators to assess the security of real installations or to compare different software products. Thus, a common practice in large organizations is to hire security experts to analyze the systems and give their opinions and recommendations. Besides being a very expensive type of assessment (that may be out of the reach for small organizations), the results obtained are very dependent on the expertise of the person (or persons) performing the assessment, which is not easy to assess.

Medium and small enterprises have limited staff and, often, the administrators have very little knowledge and feedback regarding the security implications of their decisions. In fact, although information regarding the security of many systems is commonly available, it is hardly useful for administrators that cannot take a significant portion of time and resources to do research and specialize in the topic. In this chapter we present a practical and generic methodology to collect widespread security information about the most important configuration best practices for a particular application domain. Those security-related practices can then be used to define security appraisals for three scenarios:

- **Assessing software configurations:** The list of practices can be used to derive a list of tests that allow an administrator (which may not be a security expert) to evaluate the environment he manages in terms of what are the best practices that the actual configuration of the system fulfills. This assessment allows not only a measurement of the distance of his configuration to an ideal one, but also makes him aware of important security factors (that he does not know about).
- **Assessing the capabilities of software products:** A list of security best practices associated with a particular domain allows deriving a list of security mechanisms that are expected to be part of the software that implements *some* functionality of that domain. Basically, the more security mechanisms a software product provides, the easier it is to carry out important security tasks. The idea is to create an appraisal able to evaluate how well the security mechanisms provided by a particular software help the administrator in the tasks of implementing the recommended security best practices.
- **Assessing the knowledge of system administrators:** In the very same way, a list of security practices can be used to devise tests to evaluate the security knowledge that an administrator has in a specific domain.

We present the main steps and difficulties involved in building such appraisals, and demonstrate their usefulness and feasibility by defining two specific appraisals for database installations (focusing the first two scenarios introduced above). The first one is targeted to assess the security of the configuration of a deployed database instance. We present the details of the appraisal and show its potential by evaluating, comparing and analyzing the configuration of four real installations based on four widely used DBMS (Oracle, SQLServer, PostgreSQL, and MySQL). The second appraisal is targeted to evaluate and compare out-of-the-box database software packages (which are combina-