Chapter 16

A Construct Grid Approach to Security Classification and Analysis

Michael Van Hilst
Florida Atlantic University, USA

Eduardo B. Fernandez
Florida Atlantic University, USA

ABSTRACT
This chapter presents a method of mapping solution elements to regions of the problem space. Security requires complete, effective, and comprehensive coverage. Existing methodologies can enumerate known weaknesses and common solution elements. But not every solution is right for every situation. Moreover, any weakness in any component, phase, or activity can compromise the entire system. The method presented here helps map solutions to problems, and also brings attention to what might be missing. The approach, called a construct grid, divides the conceptual problem space along multiple dimensions. The space along each dimension is defined as a continuum with identifiable regions of concern. The chapter provides examples of several dimensions and the types of concerns used to define the regions of concern.

INTRODUCTION
Security must be comprehensive. A system can be compromised by any weakness in any place at any time. To assure the security of a product or system, security must be addressed for all aspects of all components in all activities, and in every phase of the product or system lifecycle. Security must be managed top-to-bottom and beginning-to-end. However, the individual practices and mechanisms that make up a system’s security are limited in scope. Large numbers of solutions must be managed in combination to assure even basic levels of security.
The security challenge is compounded by the way real world systems are built. Consider the issues of component source in software development. Components can come from new code, open-source, runtime script, model transformation, wizard code generation, legacy application, reuse library, outsourced development, commercial-off-the-shelf, and remote web service. It is a rare and inefficient project that doesn’t leverage more than a couple of these sources.

In this chapter we present a method of surveying and analyzing coverage of the problem space. When elements of security are described in terms of the solution (encryption, authorization, authentication, etc.) it is difficult to assess the overall level and extent of protection. The solutions themselves often assume a single perspective or level of architecture, and are applied in a particular level of the organization and stage of the lifecycle. Checklists can help. But in a list, the relationships between and among the items are not expressed. In our approach, the emphasis starts with the problem as a whole. The situation is viewed from a variety of perspectives, and supports many kinds of analysis, including an analysis of gaps.

At Florida Atlantic University, our group develops security methodologies based on the use of patterns. Patterns are well known solutions to common problems in given contexts. They present both the problem and the solution in a stylized, concise and easy to read form. Patterns make it possible for practitioners looking at a specific problem or task to benefit from the experience of others in a conveniently packaged form. Patterns are collected in books, posted on the Web, and discussed in conferences. By now there are hundreds, if not thousands of patterns. Patterns are best known for their use in the field of software development. But they can be used for anything. Patterns are beginning to appear in other fields such as business management and education.

Our group, in collaboration with others around the world, produces security patterns that cover a range of concerns, including semantic and domain analysis (Delessy, & Fernandez, 2005), protection mechanisms (Fernandez, Pernul, & Larrondo-Petrie, 2008), attacks and forensics (Palaez, Fernandez, Larrondo-Petrie, & Wieser, 2007), and security architectures (Fernandez, Fonoage, VanHilst, & Marta, 2008).

In developing a methodology around the use of patterns, we faced the challenge of creating an awareness of the total security landscape and finding solutions to cover everything. While there are many solutions in the field of security, any given solution only covers a piece of the bigger problem. Given that there now exists a large and growing collection of solution patterns, how do we find an appropriate solution to a given problem, and how can we know what is covered and what is not?

In our work, we have come to the conclusion that a single end-to-end methodology, by itself, cannot realistically address all the security concerns in every situation and variation that a developer is likely to face. The variety is too great for a one-size-fits-all approach. While a systematic approach is essential, it must be augmented by the delivery of focused elements of security knowledge when and where they are needed. Patterns have proven effective for delivering focused knowledge. But choosing the right knowledge, and knowing what might still be missing, requires a broad, reflective view of the overall security situation.

The target users of this work cover a range of security stake holders. In addition to software developers, we also consider the needs and perspectives of information security managers, patterns writers, and students. Information security managers have more of a systems perspective, and an organizational perspective. Patterns writers often are looking for gaps to fill and a broader context within which to view their patterns. Students are looking to broaden their understanding of a range of security issues and perspectives.