Chapter 2
Using Security Patterns to Develop Secure Systems

Eduardo B. Fernandez
Florida Atlantic University, USA

Nobukazu Yoshioka
GRACE Center, National Institute of Informatics, Japan

Hironori Washizaki
Waseda University, Japan

Jan Jurjens
Technical University of Dortmund, Germany

Michael VanHilst
Florida Atlantic University, USA

Guenther Pernu
University of Regensburg, Germany

ABSTRACT
This chapter describes ongoing work on the use of patterns in the development of secure systems. The work reflects a collaboration among five research centers on three continents. Patterns are applied to all aspects of development, from domain analysis and attack modeling to basic design, and to all aspects of the systems under development, from the database and infrastructure to policies, monitoring, and forensics. The chapter provides an overview of the method of development involving the full range of patterns, and describes many recent contributions from the many research threads being pursued within the collaboration. Finally, future directions of research in the use of patterns are described.

INTRODUCTION
We initiated an international collaboration between our security groups a few years ago, centered on methodologies to build secure systems using patterns. We describe here where we are now and where we are going. This chapter should be considered a survey of our work and not an attempt to present new work or to introduce in detail the
Using Security Patterns to Develop Secure Systems

models presented here, for that we refer the reader to our previous publications. We also provide a section comparing our work to others but again in each paper we relate our work to others in more detail. In particular, we have worked or we are working on:

- **Secure software development methodology:** We have worked on a general methodology to build secure systems and have produced until now some specific aspects of it, which are described below. Of course, these aspects have value independently of this methodology and can be applied to other methodologies or on their own.

- **Modeling and Classification of security patterns:** We have tried to provide a precise characterization of security patterns that can be used as a basis for classification. A good classification makes the application of the patterns much easier along the software lifecycle. It also helps understand the nature and value of the patterns. Another objective is to identify which patterns are missing.

- **Misuse patterns:** A misuse pattern describes, from the point of view of the attacker, how a type of attack is performed (what units it uses and how), analyzes the ways of stopping the attack by enumerating possible security patterns that can be applied for this purpose, and describes how to trace the attack once it has happened by appropriate collection and observation of forensics data. They can be used in the lifecycle to prevent the occurrence of known types of attacks and to evaluate a completed system.

- **Characterization and selection of access control models:** Access control is a fundamental aspect of security. There are many variations of the basic access control models and it is confusing for a software developer to select an appropriate model for her application. We have defined a way to clarify their relationships and a way to guide designers in selecting an appropriate model.

- **Databases in secure applications:** Most applications need to include databases to store the persistent information, which constitutes most of the information assets of the institution. We have studied the effect of databases on the security of a system under development.

The following sections describe these aspects in detail.

**SECURE SOFTWARE DEVELOPMENT METHODOLOGY**

A good methodology for design is fundamental to produce secure systems. In Fernandez, Yoshioka, Washizaki & Jürjens (2007) we defined some requirements for such a methodology. Principles to build secure systems have been defined in some classical papers (Saltzer & Schroeder, 1975) and textbooks (Viega & McGraw, 2001), patterns may apply them implicitly. Specific requirements include:

- At each stage, there is guidance on where to apply and how to select appropriate security patterns.
- There are guidelines for pattern selection to satisfy functional requirements or restrictions at each stage.
- There are guidelines to find vulnerabilities and threats in a system.
- There are guidelines to select patterns to mitigate the identified threats.
- The models of the patterns should be relatively detailed and precise, using languages such as UML and OCL to describe the solutions.
Related Content

Modelling Information Demand in an Enterprise Context: Method, Notation, and Lessons Learned
[www.igi-global.com/article/modelling-information-demand-enterprise-context/55489?camid=4v1a](www.igi-global.com/article/modelling-information-demand-enterprise-context/55489?camid=4v1a)

SLIM: Service Location and Invocation Middleware for Mobile Wireless Sensor and Actuator Networks
[www.igi-global.com/article/slim-service-location-invocation-middleware/47038?camid=4v1a](www.igi-global.com/article/slim-service-location-invocation-middleware/47038?camid=4v1a)

Composing Systems of Systems: Requirements for the Integration of Autonomous Computer Systems
Panayiotis Periorellis (2005). *Requirements Engineering for Sociotechnical Systems* (pp. 139-152).
[www.igi-global.com/chapter/composing-systems-systems/28407?camid=4v1a](www.igi-global.com/chapter/composing-systems-systems/28407?camid=4v1a)

A Social Ontology for Integrating Security and Software Engineering
[www.igi-global.com/chapter/social-ontology-integrating-security-software/29420?camid=4v1a](www.igi-global.com/chapter/social-ontology-integrating-security-software/29420?camid=4v1a)