International Journal of Secure Software Engineering
Volume 7 • Issue 3 • July-September 2016

An Exploratory Study of the Security Design Pattern Landscape and their Classification

Poonam Ponde, Department of Computer Science, Savitribai Phule Pune University, Pune, India
Shailaja Shirwaikar, Department of Computer Science, Savitribai Phule Pune University, Pune, India

ABSTRACT

Security is a critical part of information systems and must be integrated into every aspect of the system. It requires a lot of expertise to design and implement secure systems due to the broad coverage of security issues and threats. A good system design is based on sound software engineering principles which leverages proven best practices in the form of standard guidelines and design patterns. A design pattern represents a reusable solution to a recurring problem in a specific context. The current security design pattern landscape contains several patterns, pattern catalogs and pattern classification schemes. To apply appropriate patterns for a specific problem context, a deeper understanding of this domain is essential. A survey of patterns and their classification schemes will aid in understanding pattern coverage and identifying gaps. In this paper, the authors have presented a detailed exploratory study of the security design pattern landscape. Based on their study, the authors have identified shortcomings and presented future research directions.

KEYWORDS

Classification, Design Patterns, Pattern Catalogs, Security

1. INTRODUCTION

Security is an integral aspect of information systems today. Designing and implementing secure systems requires a lot of skill and expertise. With the growing use of networked, distributed systems, applications and information, comprehensive security is not easy to achieve. Even today, it is difficult to design secure systems because of the complexity and the broad coverage of security issues. Additionally, retrofitting existing applications to security needs is more difficult. Even though the importance of security is understood and acknowledged, it is often engineered into the system at a later stage. Security concerns are not thoroughly addressed. This results in a system which is susceptible to security breaches and attacks. A good system design is based on sound software engineering principles which leverages proven best practices. Good security practices often include a list of security principles, like Viega and McGraw's (2002) ten security principles and the Open Web Application Security Project (OWASP) which provide guidelines to design secure software systems (OWASP, 2008).

In software engineering, a pattern represents a reusable solution to a recurring problem in a specific context. There are several benefits of using design patterns to design systems. The solution can be trusted since it captures expert knowledge and has been tested. Since the first security patterns described by Yoder and Barcalow (1997), this domain has evolved and several security patterns,

DOI: 10.4018/IJSSE.2016070102

pattern catalogs and classification schemes have emerged. Today, the security pattern landscape is very vast and complex. Proper organization and classification of design patterns is important. The contribution of this paper is to present the current landscape of security pattern catalogs, study their classification methodologies, identify shortcomings and present future research directions in this area.

The rest of the paper is organized as follows. Section 2 presents a literature survey of pattern catalogs. Section 3 discusses various classification methodologies developed so far. Section 4 presents previous survey work. In Section 5, we present our observations. Finally, Section 6 presents our conclusions and discusses future work.

2. SECURITY PATTERN CATALOGS

This section describes previous work on security design patterns. Christopher Alexander first introduced the concept of design patterns for use of living spaces in the book "A Pattern Language: towns, buildings, construction" (Alexander, Ishikawa, & Silverstein, 1977). The concept of pattern was later adopted for object oriented programming in the landmark patterns book for software architects, "Design Patterns: Elements of Reusable Object-Oriented Software", whose authors Gamma, Helm, Johnson, and Vlissides (1994) are known in the patterns community as the "Gang of Four" (GoF). Their book describes simple and elegant solutions to specific problems in object-oriented software design. The first design patterns related to security were published by Yoder and Barcalow in 1997. They used the GoF pattern template and presented 7 patterns namely Single Access Point, Check Point, Roles, Session, Full View with Errors, Limited View, Secure Access Layer. Subsequently, Romanosky (2001) compiled a collection of 8 design level security patterns. In a follow-up paper, 4 additional patterns were discussed in 2003. In their security patterns repository v1.0, Kienzle, Elder, Tyree and Edwards-Hewitt (2002) listed 26 patterns and 3 mini patterns. In 2004, Blakley, Heath and members of the Open Group security Forum developed a technical guide to pattern-based security design methodology and a system of security design patterns (Blakley & Heath, 2004). Their catalog contained 13 design patterns, 5 patterns for reliability, and 8 for security. The Zachman Framework (1987) is a widely used framework for enterprise system architecture. It is structured as a table which provides different system scopes and levels of abstraction in rows and different system aspects in columns. This framework has been extensively used for work on security patterns. The Microsoft Patterns and Practices group, in their document describing the Enterprise Architectural Space, extended the Zachman Framework to describe 110 patterns related to application development using the .NET framework (Trowbridge, Cunningham, Evans, Brader, & Slater, 2004). Further, Microsoft (2005) published a security patterns catalog for Web services with 18 patterns. In their book, Marcus Schumacher and a working group of security pattern experts, categorized 46 patterns into multiple categories based on the Zachman framework (Schumacher, Fernandez, Hybertson & Buschmann, 2005). Steel, Nagappan and Lai (2005) compiled a catalog of 23 core security patterns for J2EE and web services. In their paper Hafiz, Johnson and Afandi (2004) presented 9 patterns. Hafiz added 4 privacy patterns in 2006 followed by 12 patterns in 2010 (Hafiz, 2006, 2010). In their guide to Secure Design Patterns, Dougherty, Sayre, Seacord, Svoboda and Togashi (2009) at the Carnegie Mellon Software Engineering Institute described 15 design patterns. The book "Security Patterns in Practice: Designing Secure Architectures Using Software Patterns", authored by Fernandez (2013), contains 68 design patterns in 12 different categories.

A large number of patterns have emerged over the years at the Pattern Languages of Programs (PLoP) conferences around the world. The security pattern landscape today contains more than 400 security patterns. Table 1 gives a summary of the pattern catalogs.