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,
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


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.
High-Performance Modelling in Geodynamics
www.igi-global.com/chapter/high-performance-modelling-geodynamics/70616?camid=4v1a

Two Heads Are Better Than One: Leveraging Web 2.0 for Business Intelligence
www.igi-global.com/article/two-heads-better-than-one/44683?camid=4v1a