Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IMPACT FACTOR: 6.017

IJCSMC, Vol. 5, Issue. 9, September 2016, pg.222 – 228

Survey: Classification & Validation of Security Patterns in SDLC

E.R.Aruna, Associate Professor, Department of IT, Vardhaman College of Engineering
Dr. A. Rama Mohan Reddy, Professor of CSE, SVU College of Engineering
Dr. K.V. N. Sunitha, Principal and Professor of CSE, BVRIT for Women

Abstract— In software engineering, expert guidance is encapsulated in the form of security design patterns which provide reusable solutions to recurring security specific problems. More security design patterns catalogs are available and the security pattern community has produced significant contributions with this patterns, many of them are applicable to design phase. We believe it is better to explain how to use a proven methodology (Security design patterns) to design security architectures that accurately fit the needs of application design, rather than depends on a range of fixed architectures. We propose secure aware software development life cycle (saSDLC) by using the security patterns as reusable component during SDLC. In this paper we have done on classification and validation of security patterns from design phase and implementation phase since 1997 to 2016.

Keywords: secure aware SDLC, NFR, security design patterns

I. INTRODUCTION

The Security is the major concern in all software product implementations in recent years. “Security concerns must be concentrated on every phase of software development life cycle” stated by Devanbu et al [1]. It is quite difficult to do so because all the software development teams are not security experts. Security patterns contains the expert knowledge about the security concerns which will guide the software engineers in the right direction. Security patterns are proven solutions for the security problems, hence the software engineers achieves good results with nominal efforts. These security patterns are organizing as the patterns catalogs, by the time of use an engineer can select the suitable pattern and make use for the problem.

Design pattern, “describes a problem which occurs again and again in our environment and describes the core of the solution to that problem, in such a way that we can use this solution a million times over, without ever doing it the same way twice “defined by Gang of Four (GoF) authors. As these are object oriented reusable patterns, catalogs are organizing in two ways based on the purpose or scope. With respect to purpose patterns categories are creational, structural, and behavioral type patterns and based on scope object patterns and class patterns [2].

This paper is organized as Back ground of the security design patterns in section II, survey on various classifications of security patterns in section III, Representation and Validation of security patterns in section IV, and conclusion & future work in section V.

II. History of the Security Patterns

Christopher Alexander was introduced the concept of design pattern in 1997 [3]. Then these are spanned as object oriented reusable design patterns by the GoF[2]. Yoder and Barcalow were published the first security pattern in 1997. As the evolving of more patterns, the patterns are categorized into 13 procedural and 13 structural patterns and 3 mini structural patterns by Darrell M. Kienzle et al [4].

Security patterns are treated as Available System Patterns and Protected System Patterns by Blakley, B. and Heath, C et al [5]. Security patterns (cyber patterns and attack patterns) guide us to move from offhand skill to engineering discipline because they transfer knowledge about proven solutions in an understandable and reusable format to experienced users by Trowbridge et al [6].

Many security concerns, security taxonomy with related patterns and their characteristics, integrating security into system defined by Markus Schumacher et al [7]. A pattern language was defined to select all the security patterns easily by Munawar Hafiz et al [8].Nine privacy patterns and their relationships, detailed descriptions was given by Hafiz et al [9].

Fernandez et al proposed the two new classification schemes first is based on literature survey from 1997 to 2012 and the second is pattern recognition in security aspects in various domains[10]. Subsequently, more and more patterns, pattern catalogs were emerged as per security issues. Dougherty et al reported secure design patterns are descriptions, describing a general solution to a security problem that can be applied in many different situations. Rather than focus on the implementation of specific security mechanisms, these patterns are used to eliminate the accidental insertion of vulnerabilities into code or to mitigate the consequences of vulnerabilities [11].Eduardo Fernandez et al examined the structure and purpose of security patterns [12].

Many security patterns are emerged based on their domain; currently more than 400 security patterns are available. These enormous number of patterns needs to be classified. Many researchers proposed the various classification techniques based on domain specific patterns, application specific patterns, design level patterns, implementation level patterns etc. [15][16]17][18]. All of them used the pattern template most similar to design patterns for describing the security patterns.

III. Security Patterns Classifications

Some of the classifications reported by various practitioners are:

1. Hafiz et al analyzed various classification schemes for security patterns and proposed a classification scheme that uses the threat model and application context to partition patterns [13], Hafiz et al. reported classification based on the security objective, but not as domain specific [25].

2. Pattern Diagrams are used to classify the patterns by Fernandez et al [14].

3. Nobukazu yoshioka et al are categorized the security patterns are in the form of software life cycle point. Security patterns for requirement phase, design phase and implementation phase. For requirement phase security patterns are Analysis process patterns and model based patterns. The design phase patterns are pattern for specific security concern and domain specific patterns. Implementation phase patterns are secure programming guidelines, attack patterns, secure refactoring [19].

4. The well-known existing classification method of GoF classification is re-used by Konrad et al for security patterns as creational, structural and behavioral with additional level such as purpose of each pattern [20].

5. Schumacher's security patterns classification is based on Zachman's framework for enterprise architecture [21][22]. They have classified in two dimensions, first dimension is on "what","how", "where", "who", "when", and "why" interrogatives. The second dimension is different information model views such as business model or technology model and sahumacher et al added new column as security view.

6. Steel et al classify the JEE patterns as n-tire based such as web, business and web service based [23].

7. Security patterns are differentiated as architecture patterns and design patterns categories by Rosado et al [24].

8. Swiderski et al. focused on well know security acronym such as CIA (Confidentiality, Integrity and Availability) and STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation of privilege) with a total 14 patterns they have classified [26][27].

9. VanHilst et al. classified multi-dimensional matrix which addresses the problem coverage and pattern classification. The list of security concerns represented in each matrix. In this the first dimension is life cycle activities, second dimension is security patterns source [28].

10. Fernandez et al. states the architectural security patterns which are classified into two types. One type of classification is hierarchy of layers and other type is based on the relationships among the patterns. The relations among the patterns are identified using an automatic relationship extraction and analysis. This classification covers very less number of security patterns [29].
11. VanHilst et al work was enhanced by Washizaki et al by adding more dimensions for the security pattern classification. They are life cycle stage, Architecture phase, domain concern, pattern types and constraints, relations association, generalization, and aggregation [30].
12. Koen Yskout et al classified the security patterns based on the annotations, this covers the four dimensions, based on security objectives, applicability, trade-off labels and relationship among patterns [31].
13. Poonam pande et al classified the security patterns using Hierarchical Cluster Analysis, they performed cluster analysis around 211 patterns. They have identified the identical patterns and removed the redundant patterns using maximum' distance metric [32].

IV. Representation and Validation of Security Patterns during Software Development life cycle

Few researchers stated how to validate the security patterns during the design level.

1. Abramove et al have suggested the stereotype for validating the patterns during design phase [33], they have designed the data base application.

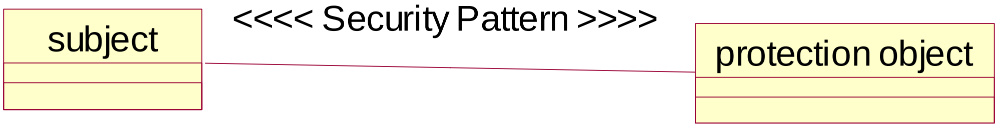

Fig1.

In Figure 1, for protecting the object while accessing by other object they are validation of security concern using the security pattern. This is only with in design level, further it is not confirming how it got evolved in the implementation phase to resolve the vulnerabilities.

2. Model checking methodology is used for verifying the composition of security patterns by Dong et al [34].

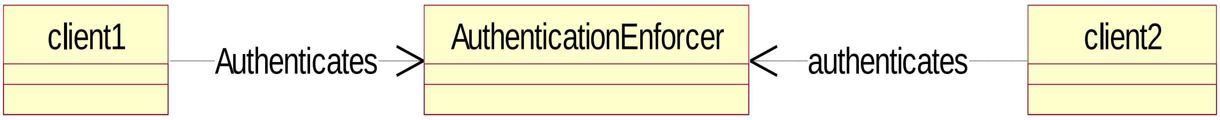

Fig2.

In Figure 2, The Authentication Enforcer pattern encapsulates the authentication logic. Here the two clients are authenticate each other by the Authentication Enforcer class. Using credentials the Authentication Enforcer class authenticates two clients and represents the authenticated user. Here also the security patterns verified at the model level, it does not guarantee that threats and vulnerabilities are resolved in the corresponding implementation code.

3. Hamid et al. proposed a method which is used to validate the application of patterns at the model level by UML They have applied the GoF mediator pattern and UML class diagram to represent air traffic controller application at design level [35] but this is also not applicable to implementation level.

4. Jan Jurjens presented extension UML allows to represent security related information with in the design diagrams.

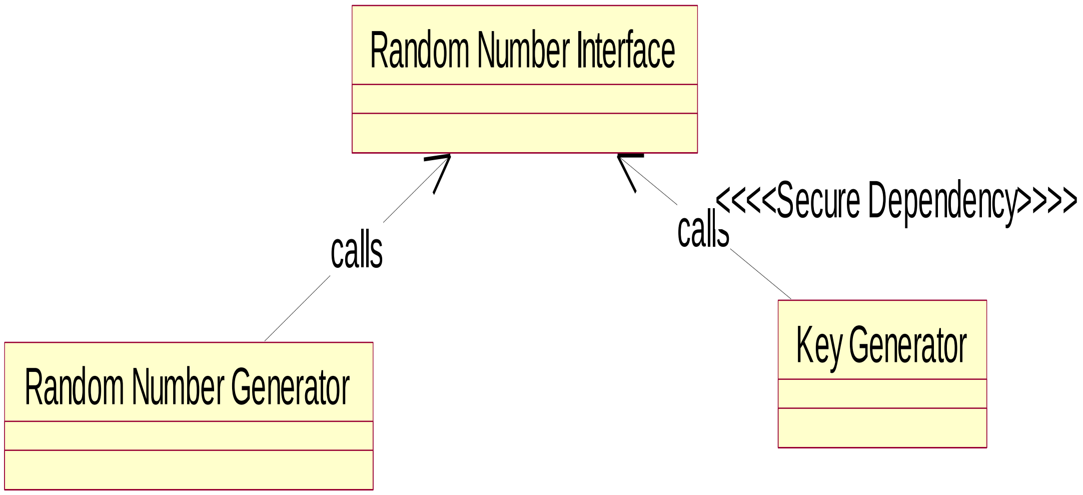

Fig3.

In Figure 3, the instances which are critical, those are representing in the stereo type, this instances are supposed to be protected [36].

5. Denis Hatebur al proposed a pattern system for security requirements engineering, this is based on security problem frames. This system produce complete description of all the sub problems solution and this will solve a complex security problem using g Jackson's problem frames [42].

6. Lodderstedt et al designing access control policies for model driven software development, this is based on Role Based Access Control (RBAC) and this model ensures the security. This model introduces the authorization constraints for granting privileges to perform operations [37].

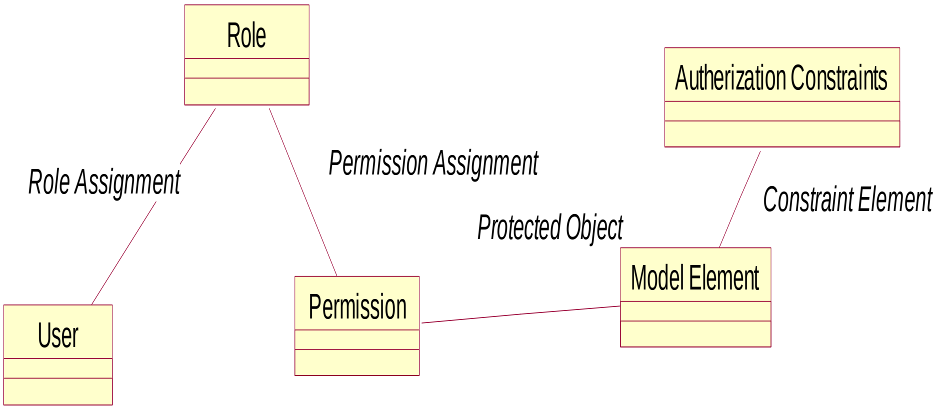

Fig.4

In figure 4, The RBAC concepts are represented as Meta models. Permission is a relative object between role and model element, here every UML model element is to take the role of protected resource.

The above two models are supporting to security concerns in modeling but they cannot be directly used at implementation level to know the correctness of the security patterns.

7. Fernandez et al proposed three patterns corresponding to most common models for security i.e. Authorization, RBAC, and Multilevel Security. These security concerns can be applied to all the levels of SDLC [38].

8. Haralambos Mouratidis et al proposed a methodology that considers security as an integral part of the whole system development process, explained through health and social care information system as a case study. This process is characterized with five key ideas considering security issues in overall development process, identify security requirements at early stage and continues until implementation stage , secondly, using Tropos hierarchical approach, third, iteration of redefinition of security requirements, fourth considering the organization security policy , fifth functional and nonfunctional requirements are defining together with clear distinction.

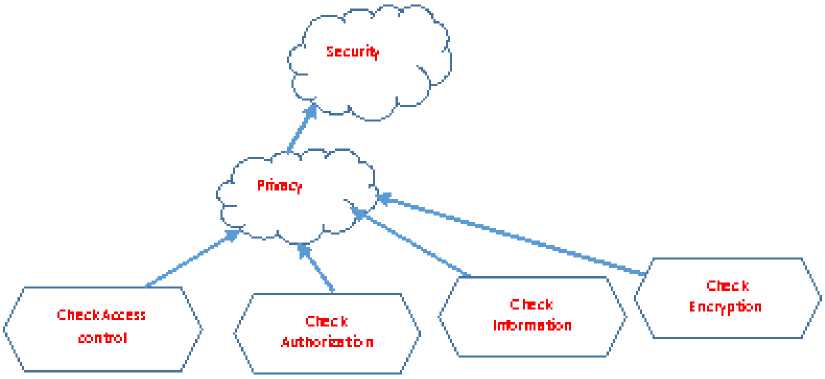

Fig 5.

In Figure 5 Designing of above nonfunctional requirements including the design of the client server application [39].They have concluded this process yet to be refined with different case studies and extensions has to be made for Formal Tropos specification language.

9. Golnaz Elahi et al proposed the extension to the i* framework for security trade-off analysis using multi-agent and goal orientation. But these models become more complex and inefficient for goal models scale and also proposed process is knowledge of security mechanisms and corresponding contributions are not existing, their work is concluded with their approach is validated with empirical studies[40].

10. Masatoshi Yoshizawa et al perform a test template to perform validation of security pattern and supported for pattern implementation. Their approach is tested for finding implementation defects and correct the defects [41].

V. Conclusion and Future Work

Most of the security pattern classification done on few patterns, these classifications are not covering all the security issues. There is no universally accepted catalog for all the security objectives. Most of the researches classified the pattern depends on the application specific, domain specific. Some researchers classified few patterns based on security objectives. There is no specific process to select the security pattern from the catalog. Some researchers concentrating on security requirements and patterns right from the inception, but there is no guarantee that identified patterns got implemented at the ending of the SDLC? Most of the researchers proposed approaches to represent the security patterns during design, but they are failed to guarantee to validate the same patterns in the implementation phase. The Security pattern template differs from one to other in certain aspects. Very few researches reported that how to use the combination of the patterns to resolve more problems.

Most of the patterns having different names with same purpose due to abstract description of the patterns. Many of the patterns serve for two or three security concerns. The presentation of security patterns during design phase does not have specific model, many of them proposed stereotypes to represent the security concerns. Very few practitioners design and validate the security patterns from design phase to implementation phase. Few researchers concentrated on the impact of security patterns on the coding and the productivity. Most of the research on security patterns is empirical study.

In future scope, the global security pattern catalog has to be emerged with all the dimensions that must be applicable for all the security concerns in the presence of all other different requirements irrespective of platform, domain or application specific. Security concerns and patterns must be identified during the inception, and the same must be representation in the design phase, must be implemented same in the construction phase and the outcome must be test with same requirement during transition phase.

By making, this as possible in future, we can include the most critical nonfunctional requirement in SDLC, this will leads to achieve secure aware SDLC.

References

[1] Dr. P. T. Devanbu, S Stubblebine, " Software Engineering for security: a road map", conference proceeding os the future of software engineering , pp.227-239,2000.

[2] E. Gamma, R. Helm,R. Johnson, and J. Vlissides, Design patterns –Elements of reusable object-oriented software, Addison-Wesley 1995.

[3] Alexander, C., Ishikawa, S. and Silverstein, M. 1977. A pattern language: towns, buildings, construction. New York : Oxford University Press.

[4] Kienzle, D. M., Elder, M. C., Tyree, D. and Edwards- Hewitt, J. 2001. Security patterns repository version 1.0. Retrieved 15 December, 2015 from http://www.scrypt.net/~celer/securitypatterns/repository.

[5] Blakley, B.and Heath, C. 2004. Security design patterns technical guide - version 1.Open Group (OG). Retrieved 24 November, 2016 from www.opengroup.org/onlinepubs/9299969899/toc.pdf

[6] Trowbridge, D., Cunningham, W., Evans, M., Brader, L. and Slater, P. 2004. Describing the enterprise architectural space. Microsoft Press

[7] Schumacher, M., Fernandez, E.B., Hybertson, D. and Buschmann, F. 2005. Security Patterns: Integrating Security and Systems Engineering. John Wiley & Sons.

[8] Munawar Hafiz, Paul Adamczyk, Ralph Johnson, "Growing a Pattern Language (for Security)", 2011.

[9] Hafiz, M. 2006. A collection of privacy design patterns. Proceedings of the 13th Conference on Patterns Language of Programming (PLoP'06)

[10] Fernandez, E. B., Yoshioka, N. and Washizaki, H. 2007. Using security patterns to build secure systems. International Workshop on Software Patterns and Quality. Information Processing Society of Japan, (pp. 47–48).

[11] Dougherty, C., Sayre, K., Seacord, R.C., Svoboda, D. and Togashi, K. 2009. Secure design patterns. Carnegie Mellon University, Software Engineering Institute, TECHNICAL REPORT CMU/SEI 2009-TR- 010.

[12] Fernandez-Buglioni, E. 2013. Security Patterns in Practice: Designing Secure Architectures Using Software Patterns. Wiley, ISBN: 978-1-119-99894-5

[13] Hafiz, M., Adamczyk, P. and Johnson, R.E. 2007. Towards an Organization of security patterns. IEEE Software, vol. 24, (pp. 52–60).

[14] Fernandez, E.B., Washizaki, H., Yoshioka, N., Kubo, A. and Fukazawa, Y. 2008. Classifying security patterns. Proceedings of the 10th Asia-Pacific Web Conference (APWEB'08).

[15] Bunke, M., Koschke, R. and Sohr, K. 2012. Organizing Security Patterns Related to Security and Pattern Recognition Requirements. International Journal on Advances in Security, vol 5 no 1 & 2.

[16] Hafiz, M., Adamczyk, P. and Johnson, R. E. 2012. Growing a Pattern Language (for security). ACM international symposium on New ideas, new paradigms, and reflections on programming and software, (pp. 139- 158), ACM New York, ISBN: 978-1-4503-1562-3.

[17] Dangler, J. 2013. Categorization of Security Design Patterns. Electronic Theses and Dissertations Paper 1119, http://dc.etsu.edu/edt/1119.

[18] Zachman, J. 1987. A framework for information systems architecture. IBM Systems Journal, 26(3).

[19] Nobukazu yoshioka et al "A survey on Security Patterns", Natinal Institute of Informatics.

[20] S. Konrad, B. H. Cheng, L. A. Campbell, and R. Wassermann, "Using security patterns to model and analyze security requirements," in International Workshop on Requirements for High Assurance Systems, 2003, pp. 13–22.

[21] M. Schumacher, E. B. Fernandez, D. Hybertson, and F. Buschmann, Security Patterns: Integrating Security and Systems Engineering. John Wiley & Sons, 2005.

[22] "The zachmann framework for enterprise architecture," 2012, last access: 23.06.2012. [Online]. Available: http: //zachma Alur ninternational.com/2/Zachman Framework.asp

[23] C. Steel, R. Nagappan, and R. Lai, Core Security Patterns: Best Practices and Strategies for J2EE(TM), Web Services, and Identity Management. Prentice Hall International, 2005.

[24] D. G. Rosado, C. Guti´errez, E. Fern´andez-Medina, and M. Piattini, "Security patterns related to security requirements," in Proceedings of the International Workshop on Security in Information Systems, 2006, pp. 163–173.

[25] M. Hafiz, P. Adamczyk, and R. E. Johnson, "Organizing security patterns," IEEE Software, vol. 24, pp. 52–60, 2007.

[26] Commission of European Communities, "Information technology security evaluation criteria, ver. 1.2," 1991, last access: 23.06.2012. [Online]. Available: https://www.bsi.bund.de/cae/servlet/contentblob/ 471346/publicationFile/30220/itsec-en pdf.pdf

[27] F. Swiderski and W. Snyder, Threat Modeling (Microsoft Professional). Microsoft Press, 2004.

[28] M. VanHilst, E. B. Fernandez, and F. A. Braz, "A multidimensional classification for users of security patterns," in Proceedings of the International Workshop on Security in Information Systems, 2008, pp. 89–98.

[29] E. B. Fernandez, H. Washizaki, N. Yoshioka, A. Kubo, and Y. Fukazawa, “Classifying security patterns,” in Proceedings of the Asian-Pacific Web Conference, Apr. 2008, pp. 342–347.

[30] H. Washizaki, E. B. Fernandez, K. Maruyama, A. Kubo, and N. Yoshioka, “Improving the classification of security patterns,” Database and Expert Systems Applications, pp. 165–170, 2009.

[31] Koen YSKOUT, “Connecting security requirements and software architecture with patterns”, thesis, 2013.

[32] Poonam Ponde, Shailaja Shirwaikar, Sharad Gore,” Hierarchical Cluster Analysis On Security Design Patterns”, ACM,*AICTC '16,* August 12 - 13, 2016, Bikaner, India.

[33] Abramov, J.; Shoval, P.; Sturm, A. Validating and Implementing Security Patterns for Database Applications. in Proceedings of the 3rd International Workshop on Software Patterns and Quality (SPAQu), Orlando, FL, USA, 25 October 2009.

[34] Dong, J.; Peng, T.; Zhao, Y. Automated verification of security pattern compositions. J. Inf. Softw. Technol. 2010, 25, 274–295.

[35] Hamid, B.; Percebois, C.; Gouteux, D. Methodology for Integration of Patterns with Validation Purpose. In Proceedings of the European Conference on Pattern Language of Programs (EuroPLoP), Irsee, Germany, 11–15 July 2012; pp. 1–14.

[36] Jürjens, J. Secure Systems Development with UML; Springer: Berlin, Germany, 2005.

[37] Lodderstedt, T.; Basin, D.A.; Doser, J. SecureUML: A UML-Based Modeling Language for Model-Driven Security. In Proceedings of the 5th International Conference on the Unified Modeling Language (UML), Dresden, Germany, 30 September–4 October 2002; pp. 426–441.

[38] Eduardo B. Fernandez and Rouyi Pan, “A pattern language for security models”, e PLoP 2001 Conference.

[39] Haralambos Mouratidis, Paolo Giorgini, Gordon Manson, “Integrating Security and Systems Engineering: Towards the Modelling of Secure Information Systems”, http://citeseerx.ist.psu.edu/.

[40] Golnaz Elahi, Eric Yu, A Goal Oriented Approach for Modeling and Analyzing Security Trade-Offs. 26th International Conference on Conceptual Modeling, Auckland, New Zealand, November 5-9, 2007. Proceedings, Springer-Verlag Berlin Heidelberg.

[41] Masatoshi Yoshizawa, Hironori Washizaki, Yoshiaki Fukazawa, Takao Okubo, Haruhiko Kaiya and Nobukazu Yoshioka, “Implementation Support of Security Design Patterns Using Test Templates”, Information 2016, 7, 34; doi:10.3390/info7020034, ww.mdpi.com/journal/information.

[42] Denis Hatebur, Maritta Heisel, Holger Schmidt, “A Pattern System for Security Requirements Engineering”, EuroPLoP '14 Proceedings of the 19th European Conference on Pattern Languages of Programs, ACM.