Volume 2, No. 4, April 2011

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

OBJECT ORIENTED DESIGN SECURITY QUANTIFICATION

Suhel Ahmad Khan[*1] and Raees Ahmad Khan[2]

*[1]Department of Information Technology, Babasaheb Bhimrao Ambedkar University (Central University), Lucknow, UP, India
ahmadsuhel28@gmail.com[1]

[2] Department of Information Technology, Babasaheb Bhimrao Ambedkar University (Central University), Lucknow, UP, India
khanraees@yahoo.com[2]

Abstract: Quantification of security at early phase produces a significant improvement to understand the management of security artifacts for best possible results. The proposed study discusses a systematic approach to quantify security based on complexity factors which having impact on security attributes. This paper provides a roadmap to researchers and software practitioner to assess, and preferably, quantify software security in design phase. A security assessment through complexity framework (SVDF) has been proposed in order to incorporate security to develop quality products. It may be used to benchmark software products according to their severity.

Keywords: Software Security; Metrics; Security Quantification; Object oriented; Complexity;

INTRODUCTION

In today's world the main challenge for decision scientists and security experts to manage software of increasing complexity. With the growing complexity, it is hard to maintain the criticality of software and increasing inadequacy at desired quality level and security become more vital, complicated and expensive. Quantitative assessment of security will provide the basis for qualitative analysis and security analysis. Software security estimation is the process of quantitative assessment of product security. Software security estimation is a complete structured process. It is required to bring down error rates at every stage of life cycle. Minimizing error rates reduces probability of failures and cost. Design phase is the first step towards problem domain to solution domain. It is the most appropriate phase to estimate security of the software. Security estimation of software in this phase will assist to protect software from loss. One of the most obvious features of science, compared say to arts and humanities is its fixation with putting number of things, by quantification using mathematical formulae. [1]

THE FRAMEWORK

As a matter of fact, researchers and practitioners highly recommend an efficient and accurate measure of software security early in design phase. There is a common consensus among industry professionals and academicians in integrating security within the development life cycle in order to deliver quality software. Unfortunately, there is no standard methodology or guideline available to quantify software security. Therefore, such a roadmap or framework, which can be followed by industry personnel and researchers to quantify security early in design phase, appears highly desirable and significant. A prescriptive framework as depicted in figure 1 (a) has been proposed to estimate security of object oriented software at design level. Moreover, security quantification figure 1 (b) has been presented in order to emphasize the importance of estimating security at design stage. The detailed description of framework is as follows:

Figure 1(b) Security quantification

Security Design & Conceptualization

Software Characterization:

A security estimation technique provides a clue to measurement severity of software. This process identifies object oriented design constructs that are used during design phase of software development and serve to define a variety of security and complexity factors. The contribution of each object oriented design characteristics is analyzed for improvement in design security.

Metric Selection:

Quantification metrics enables an application to opt for desirable security features depending on its gravity and make tradeoffs among cost, security and performance. This step is helpful to identify the relevant metrics which meet the objective of quantification of security through complexity perspective. Several metrics are available related to measurement of software at different stages of software

development life cycle. Metric selection is an important step to estimate security and complexity factors with best suited

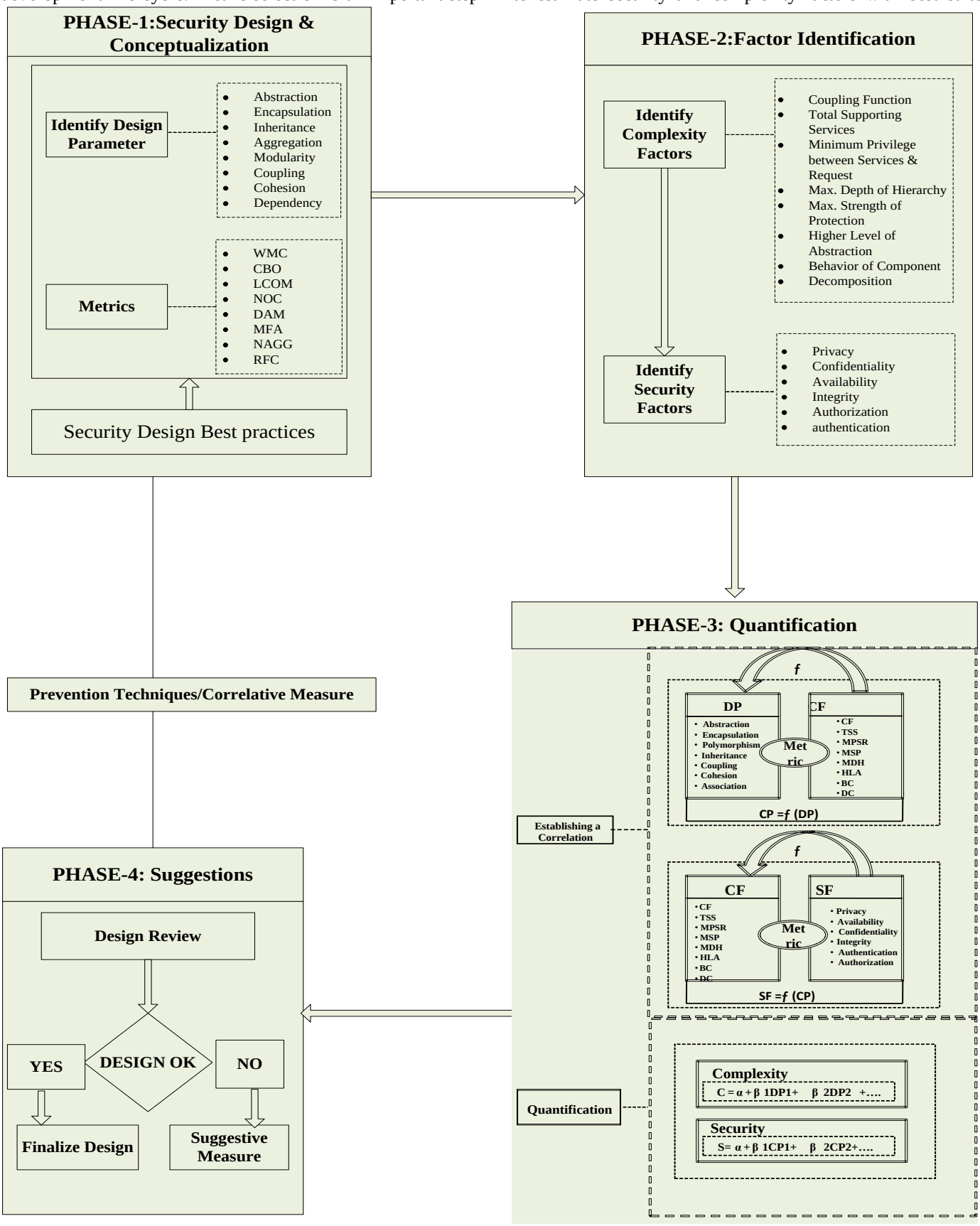

Figure 1(b): Security Assessment through Complexity Framework

results for SVDF [2, 3, 4]. In the absence of any security and complexity metric in design phase, a suite of metrics is to be proposed that may serve the purpose.

Security Design Best Practices:

This part consist a regress analysis of practical techniques and tools available for secure design practices on a special attention at design phase of software development. Security design principles are a specific type of guidelines and practices which are used to improve the security attitude of software [5]. These set of rule are applicable by proper justification with suitable results.

Factor Identification

The purpose of this step is to identify design artifacts to quantify security measures. During identification of factors which having most effect on security and complexity, a pragmatic view should be considered. If all factors and measures are considered, thus may become complicated, ineffective, or useless. Therefore, there is need to finalize factors and measures which affect the activity. Software security can be subdivided into six measurable sub characteristics or attributes: privacy, availability, integrity, confidentiality, authentication, authorization [6, 7]. It was shown in previous work that different structural properties of software design having impact on complexity factors and these identified complexity factors having impact on security attributes respectively. Security is a high level factor to software quality. In order to quantify security, its direct measures are to be identified. In this phase, the commonly accepted set of factors to complexity is to be identified [8, 9]. Design level factors will also be investigated keeping in view their impact on the overall security.

Quantification

Correlation Establishment:

A key part of the framework is divided into two parts. Part one established a correlation between complexity factors and object oriented design characteristics and later one is deal with correlation of security attributes with complexity factors. A regression line will be established between security attributes and complexity factors with the help of design metrics.

Quantification process:

Established regression will be used to quantify security factors using design metric values. Design hierarchies will be used as an input to the set formulation. Metric values are to be computed using the given hierarchy and these values are to be used to quantify security factors.

Suggestion

On the basis of the results obtained from the qualitative assessment phase, the given design is to be reviewed and revised to achieve better level of security. Design constructs are to be critically examined and may be adjusted accordingly in order to achieve the index value.

Design Review:

On the basis of the quantitative values obtained, a qualitative assessment of security factors is performed. A contextual finding will be discussed and used for review and revision of the given design. This phase will help in benchmarking software products according to their security.

Suggestive Measures:

A regress analysis is performed at this stage to avoid all discrepancies of design and add prevention techniques to resolve the incorrect design issue.

Finalize Design:

Finalization of best design & metric suite is the last step of the security quantification process. During this process, the optimal solution is achieved in the set of best possible design & metric suit that are related to the relevant measures directly and indubitably, selected and verified.

CONCLUSION

Security estimation of software must be a mandatory feature of software at early stage of development life cycle. Unifying security attributes, models, metrics and software characteristics, security estimation is possible at the early stage of software development life cycle. For security estimation mechanism, there is need to develop efficient security metrics for complexity perspective to evaluate design complexity more accurately.

ACKNOWLEDGEMENT

This work is sponsored by University Grants Commission (UGC), New Delhi, India, under F. No. 34-107\2008 (SR).

REFERENCES

[1] http://www.calresco.org/lucas/quatify.htm
[2] S. R. Chidember and C. F. Kemerer, “Towards A Metric Suite for Object Oriented Design”, OOPSLA’91, ACM, pp:197-211.
[3] Jagdish Bansiya, Carl G.Davis, “A Hierarchical Model for Object Oriented Design Quality Assessment” IEEE Transaction on Software Engg, Vol 28, No. 1, 2002
[4] R.A. Khan, K. Mustafa,“Metric Based Testability Model for Object Oriented Design(MTMOOD)”, SIGSOFT Software Engg. Notes, Vol. 34 Number 2,March 2009
[5] P. H. Meland, J. Jenesen, “Secure Software Design in Practice”, ARES.2008, IEEE, 0-7695-3102-4/08 © IEEE.
[6] C. Wang and W.A. Wulf, “A framework for security measurement” Proc. of National Information Systems Security Conference, 7-10 Oct 1997, pp: 522-533.
[7] B. B. Madan, Trivedi, “Modelling and Quantification of Security Attributes of Software Systems”, Dependable Systems and Networks DNS’022, IEEE.
[8] G. Booch, “Object Oriented Analysis and Design with Application”, Addison Wesley, 3rd Edition, ISBN-0-201-89551-X
[9] Suhel Ahmad khan and R.A. Khan, “Securing Object oriented Design: A Complexity Perspective”, International

Journal of Computer application, Volume 8, No 13, Oct 2010, pp. 8-12.

