Indian Journal of Science and Technology, *Vol 9(29), DOI: 10.17485/ijst/2016/v9i29/89280, August 2016*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Model to Quantify Integrity at Requirement Phase

Parveen Nikhat[1*], Nayak Sandeep Kumar[1] and M. H. Khan[2]

[1]Department of Computer Application, Integral University, Kursi Road, Dashauli, Lucknow - 226021, U.P., India;
nikhat0891@gmail.com, nayak.kr.sandeep@gmail.com
[2]Department of Computer Engineering, I.E.T, Sitapur Road, Lucknow - 226021, Uttar Pradesh, India;
mhkhanietfaculty@gmail.com

Abstract

Objectives: The software security and its proper measurement involve various tools and techniques. To make software secure its foundation stone, the requirement, should also be secure and therefore the integrity control for requirement at the same phase became the objective for delivering secure requirement and so forth the software. **Method/Analysis:** The past research study entails about less secure software deliver by industries and among the major cause of security lacking, one cause is integrity to requirements. Requirement integrity can be observed as trustworthy, complete and veracity requirement for producing secure software. Only conceptual notion of integrity is not capable to make any component secure but it must be depicted in understandable and quantifiable idiom for assessing the better security solution to requirement and therefore to software. **Findings:** MQI^R (Model to quantify integrity) for requirement at requirement phase of software development process is a new assessment technique that tries to satisfy all major constraints regarding secure requirements and so forth for software. To implement this new technique a relevant set of values in terms of input is captured for proper data management from various live projects under going in some software companies of repute. An appropriate quantification of requirement data is also furnished for sufficient checking of security level and its efficiency. The technique has also been validated through capturing online shopping data so that its implications may also be assessed accurately. **Novelty/Improvement:** As far as the application of this technique (MQI^R) is concern, the article emphasis on complete usability of online functioning at its highest level of integrity that maintains security with the boundary conditions of e-commerce.

Keywords: Integrity, Requirement Traits, Security Attributes, Security Estimation and Integrity Model

1. Introduction

The biggest challenge by software professionals is to build secured software. Various integrity requirements are available for software organizations which are qualitative, but for accurate estimation it is necessary to have measurable requirements[1]. To compute security it is better to analyze requirement constructs by means of security pillars that can be considered as availability, confidentiality, and integrity. By accomplishing such implementation, this possibly will facilitate security experts to reduce security flaws right from beginning of the software development.

CERT has developed SQUARE methodology that emphasizes on needs and its acceptation of residing security requirements well in advance[2]. According to a survey on security perspectives it was revealed out about the software that minimum security features hold sixty percent of higher business threat as compared with the software that are already secured. The studies reveal the truth that secure software knows how to divaricate significantly according to user requirement, updated design and its implementation[3,4].

2. Addressing Integrity Requirement at Initial Phase of Software Development

Security demands that integrity information should provide an assurance as the data must be authentic and

*Author for correspondence

complete[5]. Traditionally data integrity has been maintained by security models based on the physical behavior of the requirement specifications. These specifications can be formalized by requiring data correctness[6].

Integrity can easily be captivated if unauthorized person performed any changes either intentionally or accidentally to the system. Loss of integrity lead to incorrect data and if it is not recovered quickly then the decision made by the software results inaccurate and erroneous. To avoid integrity breach in initial phase of software development that is requirement stage, the developer must ensure about the appropriate modification done on data that has occurred in data structure. Any secure communication must allow trusted mechanism such as authorization or authentication in order to process complete and secure operation. The completeness of requirement should be incorporated in order to ensure the traceability and Unambiguity of requirement.

3. Security Quantification

Assessment of security can be performed through quantification and there are different methodologies and approaches available which are either theoretical or best practices with respect to implement security[7, 8]. At any circumstances if unnecessary requirement violates the security, it gives negative impact to its acceptance level. Security quantification will help the software developer to achieve the security goals and cut down the cost of reuse. An integrity model is anticipated in order to quantify security at requirement time so as to clarify the relationship between requirement and security. The principal objective of model has been used to classify the qualitative features of security metrics that can assess through requirement perspectives.

4. Establish a Relation between Security Attributes and Requirement Parameters

For any secure software, the three basic security pillars considered are: confidentiality, integrity and availability[9]. A number of security metrics are surviving during system level or design level. Hackers try to identify the inaccuracy of the system through which they make the system insecure and hence exploit it. Researchers and developers have observed that the weaknesses are generally found during design time of software development. To remove weakness from software during design time, it is mandatory to gather secure requirement at early stage of development. The fundamental requirement constructs are examining Unambiguity, complete, understandable and traceable quality characteristic with respect to SATC's attributes[10-12]. Metrics are helpful to maximize/control the attributes of an entity. In order to increase potency of metrics related to security approach with relevant to requirement parameters are taken from[13,14]. To increase maximum efficiency of protection at requirement time, it is requisite to remove ambiguity and volatility at any stage of the requirement which ruled out unnecessary privileged of services.

Figure 1 illustrates the importance of study in order to establish a contextual relationship between requirement attributes and security factors such that security can be quantified with available set of requirements.

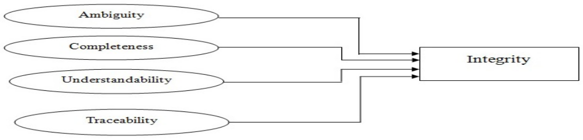

Figure 1. Relation Diagram.

5. Model Development to Quantify Integrity

To evolve protective quantification model from requirement perspectives, standard quality models have been considered on this basis[15-17]. The following steps are involved in order to develop model to quantify integrity at requirement phase (MQI^R).

- Recognition of quality factors that control integrity at requirement phase.
- Identify requirement characteristics.
- Establish correlation between them.

The relationship between the security factors and requirement attributes are based on virtual importance of individual factors which shows a major effect on security at requirement time that directly correlate the quality traits and is proportionately evaluated. The coefficient is acquired with the help of multiple linear regression line. Multiple regression equation is established with association shown among the data variables as dependent data and multiple independent data. Thus the equation may represent the way as follows:

$$Y= m1\ X1 + m2\ X2 + \ldots\ldots\ldots\ldots.. + mnXn + b \qquad (1)$$

where

- Y represents dependent data variable,
- The independent data variables Xs are associated to Y and are presume to elucidate the variation in Y which is plotted on X axis.
- The m1, m2,……,mn is the slope of line in equation that represents regression coefficients of individual independent data variables.
- And b is the y- intercept.

Taking into examination as similar, an equation has been established in order to quantify integrity of requirement. A requirement use case structure of Online Banking System is depicted in Figure 2 to quantify integrity. The seven versions of requirement structure diagram are being depicted for evaluating measured value which is illustrated in Table1. The data requisite for accepted integrity values is being used from [18]. The multiple linear regression models are integrated for the smallest set of integrity metric and its conclusion is depicted in equation (3).

$$\text{Integrity} = b+m1 * AR + m2 * CR + m3 * UR +m4 * TR \tag{2}$$

$$\text{Integrity} = -.201+ .563 *AR -.137 * CR +.082 * UR + 1.186 * TR \tag{3}$$

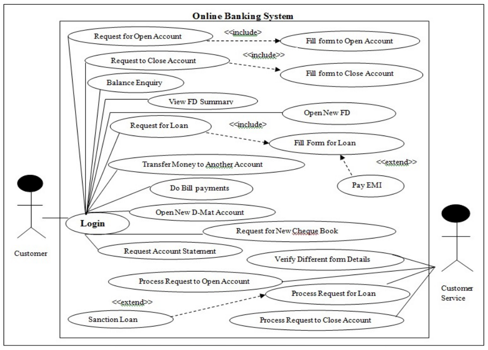

Figure 2. Online Banking System Use Case Diagram.

An analysis of deliberated data of an integrity model is stated in Table 1 is related with the statistical justification of used data that signifies the high impedance value of R Square illustrated that integrity model is highly efficient. The result is tabulated in Table 2 in order to elucidate the correlation analysis for quantify integrity, which represent for the total System, in which all of the requirement constructs are acquainted vigorously correlated with integrity. The requirement constructs AR, CR, UR and TR are Ambiguity Requirement, Completeness Requirement, Understandability Requirement and Traceable Requirement respectively.

Table 1. Summary of Model.

Mode	R	R Square	Standard Error
1	.993	.987	0.014

Table 2. Integrity Computation Table.

Requirement Diagram	Standard Integrity	AR	CR	UR	TR
RD1	0.894	0.13	0.781	0.887	0.893
RD2	0.921	0.21	0.887	0.75	0.897
RD3	0.961	0.153	0.89	0.682	0.957
RD4	0.83	0.126	0.824	0.611	0.877
RD5	0.786	0.23	0.74	0.653	0.765
RD6	0.811	0.113	0.742	0.573	0.838
RD7	0.753	0.143	0.838	0.779	0.777

6. Validation of Model through Statistical Analysis

The feasible examinations are beneficial to validate proposed integrity model in order to set up its efficacy for realistic use. A trial examination for proposed integrity model namely Model to quantify integrity (MQI^R) at requirement phase has been performed for validating using sample tryouts. The specifics of validation and data regarding integrity formulation is performed for ten version of requirement diagram based on online shopping system shown in Figure 3 and the calculated data is represented in table 3.

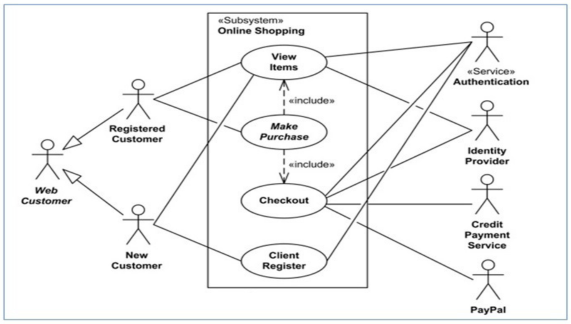

Figure 3. Online Shopping Use Case Diagram.

For any acceptance of proposed model it is mandatory to check the criteria of accuracy. A 2-tail student sample test has been instigated to analyze the dissimilarity between two population means i.e., standard integrity and computed integrity values. In Table 4 the 2-t test examination of integrity model values is depicted.

Table 3. Integrity Estimation

Requirement Diagram	AR	CR	UR	TR	Standard Integrity	Computed Integrity
RD1	0.11	0.783	0.787	0.913	0.870	0.961
RD2	0.121	0.687	0.85	0.797	0.702	0.812
RD3	0.173	0.879	0.782	0.857	0.873	0.891
RD4	0.216	0.924	0.631	0.9543	0.879	0.923
RD5	0.123	0.834	0.753	0.865	0.889	0.904
RD6	0.164	0.735	0.673	0.788	0.687	0.713
RD7	0.187	0.738	0.877	0.7786	0.583	0.778
RD8	0.157	0.835	0.657	0.833	0.739	0.802
RD9	0.119	0.878	0.786	0.737	0.661	0.795
RD10	0.197	0.793	0.777	0.897	0.735	0.883

Table 4. 2-t Test for Integrity

	No. of Samples	Mean Value	Std. Div. Value
Standard Integrity	10	0.762	0.109
Computed Integrity	10	0.846	0.077

t Score= 1.99
P (Two Tailed) value = 0.062
Correlation Coefficient=0.834

Null hypothesis (H0): It is stated that there is no significant difference between standard integrity and computed integrity.

H0: µ1-µ2 = 0

Alternate hypothesis (HA): It is stated that there is significant difference between standard integrity and computed integrity.

HA: µ1-µ2 ≠ 0

In the above hypothesis µ1 and µ2 are treated as sample means of population. Mean value and Standard Deviation value have been computed for specified two samples and represented in Table 4. Pearson correlation coefficient comes out to be 0.834, that shows the standard integrity and computed integrity is highly correlated. The hypothesis is tested with level of significance of 0.05. The p value is 0.062. Hence, the acceptance of null hypothesis directly discards the alternate hypothesis. Therefore relation used for integrity computation is accepted.

7. Conclusion

A Model (MQI^R) has been developed to quantify integrity from requirement perspective at the initial stage of development of software. It estimates the integrity with reflect to requirement parameters which are influenced according to their weight. A multiple linear regression method is carried out to quantify the model. The early quantification signifies the quality of software at the early stage of SDLC. Hence quantification of integrity enhance the security at the initiation of the software i.e., at requirement phase. The projected model has been validated and statistical analysis implies the acceptance of the model.

8. References

1. Pfleeger, Shari Lawrence, and Robert K. Cunningham. Why Measuring Security Is Hard. Co-published By The IEEE Computer And Reliability Societies. 2010; p. 46-54.
2. CERT. Date accessed: 02 May 2015: Available from: http://www.cert.org.
3. Flechais, Sasse M and Hailes SMV. Bringing Security Home: A Process for developing secure and usable systems, NSPW'03. ACM. 2003 August; p. 18-21.
4. Madan BB, Popstojanova KG, Vaidyanathan K and Trivedi KS. A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant System. Elsevier: An International Journal of Performance Evaluation. 2004; 56:167-86.
5. Nikhat Parveen, Md Rizwan Beg, et al. Software Security Issues: Requirement Perspectives. International Journal of Scientific & Engineering Research. 2014 July; 5(7):11-15. ISSN 2229-5518.
6. Li Peng, Yun Mao, et al. Information Integrity Policies. Date accessed: 5 Mar 2015: Available from: www.cis.upenn.edu/~stevez/papers/LMZ03.pdf.
7. Chandra S and Khan RA. Software Security Metric Identification Framework (SSM). International Conference on Advances in Computing, Communication and Control, ICAC3'09. ACM. 2009.

8. Se-Yun Kim, Seong Taek Park, Mi Hyun Ko. Analysis of the Competencies of Information Security Consultants: Comparison between Required Level and Retention Level. Indian Journal of Science and Technology. 2015 Sep; 8(21). DOI: 10.17485/ijst/2015/v8i21/79119.
9. Walton GH, Longstaff TA, Linder RC. Computational Evaluation of Software Security Attributes. IEEE. 1997.
10. Available from: http://www.sqa.net/softwarequalitymetrics.html.
11. Parveen Nikhat, Md Rizwan Beg and Khan MH. Bridging the Gap between Requirement and Security through Secure Requirement Specification Checklist. Pune, India: Proceedings of 16th IRF International Conference, 14th December 2014. p. 6-10. ISBN: 978-93-84209-74-2.
12. Shahid Iqbal and Naeem Ahmed Khan M. Yet another Set of Requirement Metrics for Software Projects. International Journal of Software Engineering and Its Applications. 2012; 6.1:19-28.
13. Bokhari Mohammad Ubaidullah and Shams Tabrez Ubaidullah Siddiqui. Metrics for Requirements Engineering and Automated Requirements Tools. Proceedings of the 5th National Conference, INDIACom-2011.
14. Ali Mohammed Javeed. Metrics for Requirements Engineering. 2006. Available from: www.cs.umu.se/education/examina/Rapporter/JaveedAli.pdf.
15. Chandra S and Khan RA. Software Security Metric Identification Framework (SSM). International Conference on Advances in Computing, Communication and Control, ICAC3'09. ACM. 2009.
16. Wang C and Wulf. A Framework for Security Measurement. Proc. National Information Systems Security Conference. 1997 Oct 7-10; p. 522-33.
17. Subramaniam Hema, Zulzalil Hazura, Marzanah A Jabar, Saadah Hassan. Feasibility Study of Aspect Mining at Requirement Level. Indian Journal of Science and Technology. 2014 Jan; 7(5). DOI: 10.17485/ijst/2014/v7i5/49471.
18. Chandra S, Khan RA. A Methodology to Check Integrity of a Class Hierarchy. International Journal of Recent Trends in Engineering. 2009 November; 2(4):83-85.