American Journal of Software Engineering and Applications
2015; 4(5): 86-91
Published online September 24, 2015 (http://www.sciencepublishinggroup.com/j/ajsea)
doi: 10.11648/j.ajsea.20150405.12
ISSN: 2327-2473 (Print); ISSN: 2327-249X (Online)

Model to Quantify Availability at Requirement Phase of Secure Software

Nikhat Parveen[1], Mohammad Rizwan Beg[1], M. H. Khan[2]

[1]Department of Computer Application, Integral University, Lucknow, India
[2]Department of Computer Engineering, Institute of Engineering and Technology, Lucknow, India

Email address:
nikhat0891@gmail.com (N. Parveen), rizwanbeg@gmail.com (M. R. Beg), mhkhan.ietfaculty@yahoo.com (M. H. Khan)

To cite this article:
Nikhat Parveen, Mohammad Rizwan Beg, M. H. Khan. Model to Quantify Availability at Requirement Phase of Secure Software. *American Journal of Software Engineering and Applications*. Vol. 4, No. 5, 2015, pp. 86-91. doi: 10.11648/j.ajsea.20150405.12

Abstract: A number of security mechanisms are available to protect data such as digital signature, audits log, encryption, refining etc. however they completely not able to stop malevolent attacks. Hackers and attackers continuously try to exploit security which can be easily pushed through loopholes that are available at users end. The core reasons for such problem are mainly generated by terrible software requirements which are implemented without proper analysis of risks and threats. In order to reduce vulnerabilities security requirements standards, policies are tightly bound and used right from the beginning of software development. The major purpose of security standards and policy is to ensure that the data is always available at random in order to support security requirements against identified risks. The focus on this paper is to propose a model to quantify availability (MQA^R) by using multiple regression technique at requirement phase. To rationalize the model statistical data is used to validate assess availability at requirement level and the significance of this study concludes that the calculated data is highly acceptable.

Keywords: Software Security, Requirement Attributes, Security Quantification, Availability Quantification Model

1. Introduction

The world is moving rapidly to be Hi-Tech and it is totally dependent on computer and internet of things (IOT). Most of the computer and internet services facilitates user with online services. Such services lie on the network platform in order to provide facility to end user without placing any restrictions. This is the fact that unsecured requirement will lose the reliability of the system and hence breaches security. The trait of availability with respect to software security may intentionally pose to deny access to services by making it unavailable. Such actions behave to protect sensitive data from security breaches. For example session duration play important role to maintain availability of services, as the session expire the data becomes unavailable. Security experts believed that incorporating security at an early stage of development will reduce flaws, vulnerabilities and unwanted data at requirement time.

Availability behaves as fraction of instance that a produced system is functioning adequately. It is the extent to which the information is accessible and functional. Denial of services makes system's service unavailable for unauthorized users [1, 2]. Availability ensures that services are available for authorized user and it is operational when they are needed. It is suggested that to improve security, security policies and measures must be incorporated during requirement phase to eliminate vulnerabilities. For an outfitted design, all functional requirements must be available to serve its purpose. Availability and reliability are often interrelated to each other [3]. Software reliability measures possibility of error free services that are intended by the software for specified interval under stated conditions. Rap tool is used to appraise reliability and availability of software, which consists of three phases: the first phase defines reliability and availability goals; second phase transforms goals into architectural elements and third phase represent these elements in architectural models and perform evaluation in order to verify that the resultant architecture is satisfying the requirements or not[4].This is true that reliable software has high availability but available software may or may not be reliable.

2. Availabily at Requirement Phase

Setting availability goal is a complex process. For any software system to provide its services, the information

must be available whenever it is needed. Such actions confirm that the processing of information must be correct and reliable. This reliable information must be protected by providing minimum privilege services in order to avoid ambiguity so that the available information can be secured. This is the fact that if information is available at high priority, the security reluctantly decreases. However securities of services need adequate protection in the form of physical security which behaves as fundamental security precaution and it is essential for the system to meet the user's availability requirements.

The three basic security requirements confidentiality, integrity and availability namely CIA has been acknowledged. CIA being the cornerstone of security and it totally depends on authentication and authorization [6]. On account of user's authentication and authorization level, system services are provided to authorize user only. For any decisive system if data is unavailable, it will directly affect the functionality of the system. To avoid unavailability at requirement phase, it is mandatory to make a proper adjustment of occurrence for document structure. Secure transmission at requirement time allows trusted authorization or trusted authentication mechanism to process operation. This can be incorporated with completeness of requirement that ensure the traceability and Unambiguity of requirement which could not disclose any information at any given time. These can be evaluated by direct measurement of attributes of requirement which includes ambiguity, completeness, understandability, traceability which all influence the availability as security at requirement time.

3. Building Correlation Between Security Attributes and Requirement Parameters

An estimation of security can be evaluated through quantification which helps to assess the cost and effort made by developers in order to secure software. Accurate and precise results are only generated through quantification. After lots of scrupulous discussion on security quantification concluded that a negligible effort has been done during requirement time. Many procedures and technique are based on either theoretical or best practices that can implements security [7]. The unwanted requirement violates the security and gives negative impact to its acceptance level. The study shows that whenever the requirement is gathered to design any software, this should be kept in mind that the ambiguity and volatility of the requirement will be minimize in order to increase security. For any information when it is shared, it increases the availability of same information but due to any vague or modified session information gets tampered [8]. Probability of remains accessible for data is always not valuable from security perspective. For example, in online banking system if the data is available for longer period, it is easy to breach the security but due to session expired the data becomes unavailable and thus increases security. Impact of some requirement constructs on security attributes has been shown in table 1. The requirement constructs ambiguity and volatility has negative impacts on security whereas requirement constructs completeness, understandability and traceability have positive impact on security which is shown by downward arrow and upward arrow respectively.

The best time to incorporate security issues is at requirement time. To better understand the relationship between requirement and security a correlation has been established and model is proposed for quantification of security at requirement time. The primary objective is to identify the qualitative metrics for security estimation through requirement perspectives.

Information security plays an important role while developing safe and sound software. Several security metrics are available at system level or design level. Attackers try to identify the weakness of the system and exploit them. It has been observed that the weakness can be found during design time of software development. In order to remove weakness from design time, it is required to gather secure requirement. The core requirement constructs are Unambiguity, completeness, understandability and traceability with respect to SATC's attributes [9], [10], [11]. The metrics are helpful to maximize/control the security perspective with respect to requirement parameters are taken from [12], [13]. To increase maximum potency of protection at requirement time, it is mandatory to remove ambiguity and volatility of the requirement that avoid unnecessary authorization of services. The significance of this study is to quantify security with synchronized set of requirement attributes which is depicted as relation diagram in Fig 1.

Table 1. *Impact of requirement constructs on security attribute.*

Requirement Constructs /Security Attributes	Access Control	Authenticity	Availability	Confidentiality	Integrity	Non-Repudiation
Ambiguous	↓	↓	↓	↓	↓	↓
Completeness	↑	↑	↑	↑	↑	↑
Understandability	↑	↑	↑	↑	↑	↑
Traceability	↑	↑	↑	↑	↑	↑
Volatility	↓	↓	↓	↓	↓	↓

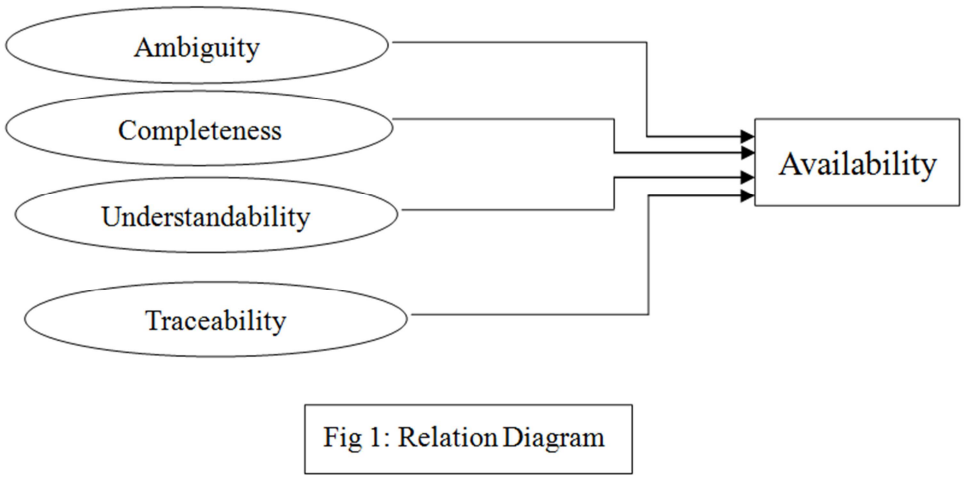

Fig. 1. *Relation Diagram.*

4. Model Development to Quantify Availability

The generic quality models have been considered as a basis to develop security quantification model from requirement perspectives [5], [14], [15]. Model to quantify availability at requirement phase (MQAR) the following steps are involved.

- Identification of quality factors that influence availability at requirement phase.
- Identification of requirement characteristics.
- Develop correlation between them.

Based upon the relationship between the security factors and requirement attributes, a relative significance of individual factors shows a major impact on security at requirement time which influence the quality attribute and is proportionally weighed. A multiple linear regression is used to get the coefficients. The regression established a relation between dependent variables and multiple independent variables. Thus the multiple regression equation may get the form as follows:

$$Y= \alpha +\beta 1\ X1 + \beta 2\ X2 +\ldots+ \beta n\ Xn \qquad (1)$$

where

- Y is dependent variable,
- The Xs are independent variables related to Y and are expected to explain the variance in Y.
- The βs are the regression coefficients of the particular independent variables. Regression coefficient represent average amount of dependent increase/decrease when the independents are held constants.
- And α is the intercept.

The multiple linear regression models are fitted for the minimal set of availability metric and result is shown in equation (3).

$$Availability=\alpha+\beta 1*AR+\beta 2*CR+\beta 3*UR+\beta 4*TR \qquad (2)$$

$$Availability=-.273-.777*AR+.458*CR+.253*UR+.826*TR \qquad (3)$$

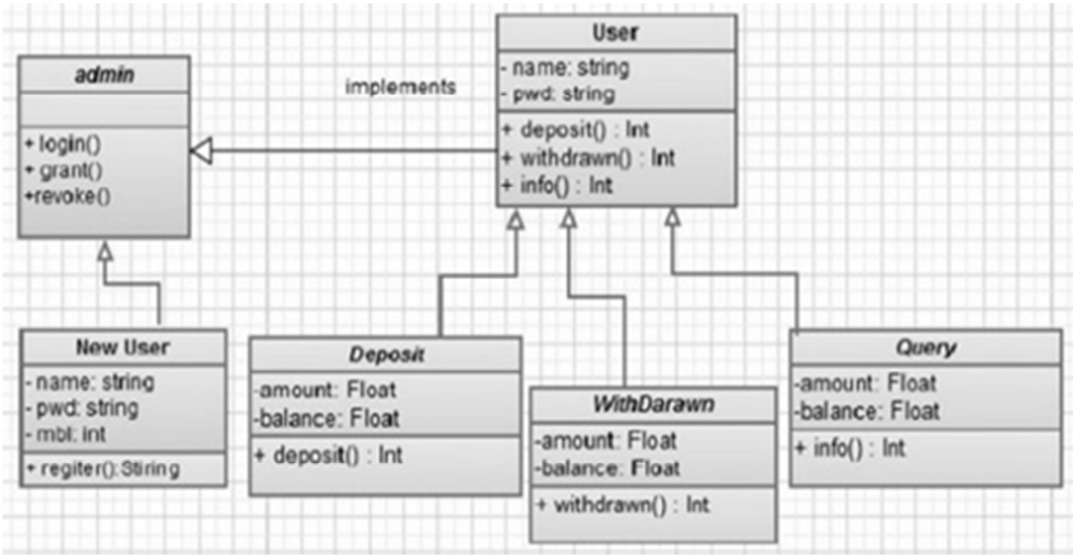

Fig. 2. *Online Banking System.*

Ambiguity Requirement (AR), Completeness Requirement (CR), Understandability Requirement (UR) and Traceable Requirement (TR) incorporate the quality requirement of software. Taking deliberators for the same, multiple regression equation to quantify availability of requirement has been established. A requirement hierarchy of Online Banking System is depicted in Fig: 2. has been presented to quantify availability. The seven versions of requirement hierarchies diagram are being used for metric value depicted in Table1 and data needed for standard availability values is taken from [16].

The model summary of deliberated data is mentioned in Table 2 which imparts the statistical elucidation of used data and signifies the high value of R Square represents that model is highly effective. Table 3 summarizes the outcome of the correlation analysis for quantify availability, and shows that for all the System, all of the requirement constructs are strongly correlated with security as availability.

Table 2. *Summary of model.*

Model	R	R Square	Standard Error	Significance F Change
1	.922	.850	0.051	0.276

Table 3. *Availability computation table.*

Requirement Diagram	Standard Availability	AR	CR	UR	TR
RD1	0.894	0.133	0.881	0.867	0.793
RD2	0.921	0.121	0.787	0.85	0.877
RD3	0.961	0.23	0.839	0.782	0.957
RD4	0.83	0.116	0.724	0.711	0.837
RD5	0.786	0.21	0.84	0.653	0.865
RD6	0.811	0.113	0.772	0.673	0.738
RD7	0.753	0.158	0.633	0.879	0.777

5. Validation of Model

The viable experiments are useful to validate proposed model in order to establish its effectiveness for practical use. Therefore, an experimental validation of the proposed model namely Model to quantify availability (MQAR) at requirement phase has been carried out using sample tryouts. The details of validations and data regarding availability formulation is carried out for ten version of requirement hierarchy diagram of online shopping system in Fig.3 and the estimated data is shown in table 4.

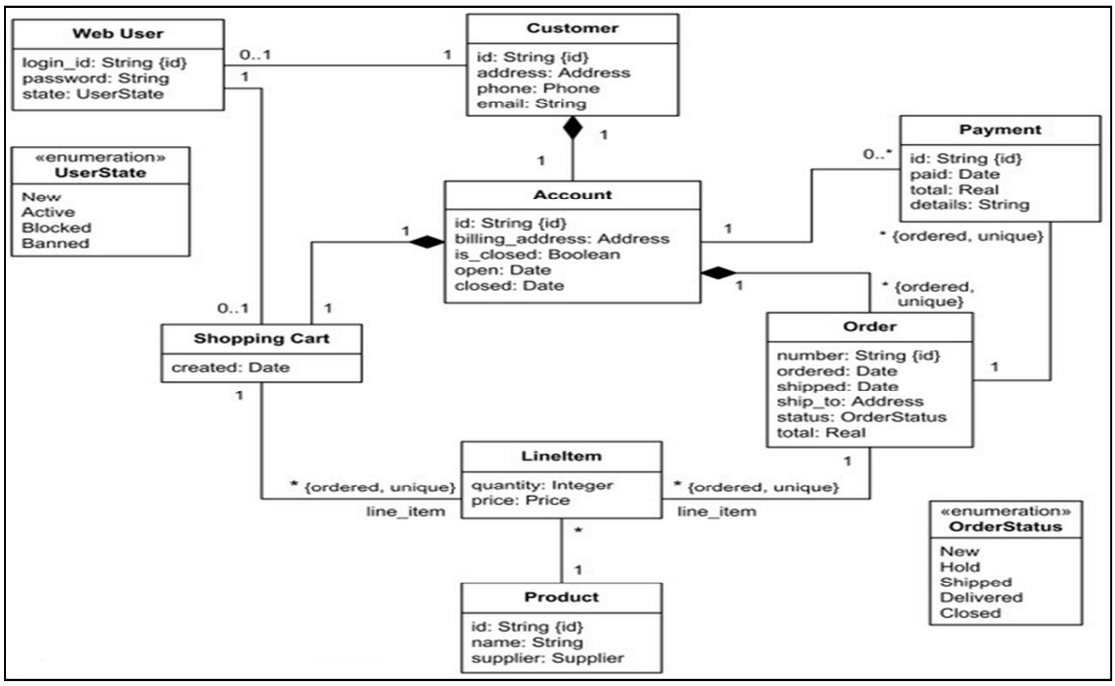

Fig. 3. *Online Banking System.*

Table 4. *Availability estimation.*

Requirement Diagram	AR	CR	UR	TR	Standard Availability	Computed Availability
RD1	0.113	0.883	0.667	0.893	0.847	0.950
RD2	0.171	0.777	0.875	0.897	0.879	0.912
RD3	0.127	0.679	0.832	0.877	0.863	0.874
RD4	0.116	0.834	0.731	0.893	0.928	0.941
RD5	0.133	0.754	0.673	0.875	0.836	0.862
RD6	0.18	0.835	0.773	0.878	0.711	0.890
RD7	0.167	0.738	0.677	0.886	0.753	0.838
RD8	0.197	0.897	0.757	0.933	0.801	0.947
RD9	0.133	0.768	0.886	0.837	0.811	0.891
RD10	0.12	0.874	0.837	0.897	0.934	0.987

It is compulsory to check the validity of proposed model for acceptance. A 2-tail sample test has been initiated to test the difference between two population means i.e., standard availability and computed availability values. The t test observation of availability values is shown in table 5.

Table 5. *T test for availability.*

	N	Mean	Std. Div.
Standard Integrity	10	0.836	0.071
Computed Integrity	10	0.909	0.046
t Statistic= 2.72			
P value = 0.014 (Two Tailed)			
Conclusion: Accept Alternate Hypothesis			

Null hypothesis (H0): There is significant difference between standard availability and computed availability.

Alternate hypothesis (HA): There is no significant difference between standard availability and computed availability.

$$H0: \mu1-\mu2 = 0 \text{ verses } HA: \mu1-\mu2 \neq 0$$

where μ1 and μ2 are the sample population means and '0' (zero) is the hypothesized difference between the two sample population means. Mean and Standard Div have been computed for given two samples and shown in Table 4. The hypothesis is trusted using 95% confidence. The p value is 0.014. Hence, null hypothesis is rejected and alternate hypothesis is accepted. Therefore the equation used in requirement parameter for availability computation is highly accepted.

6. Limitation of Study

Every coin has two sides. In research point of view both surfaces hold crucial position. However optimistic appearance offer new dimensions to proposed study while pessimistic portion highlights the deficiencies of work. The approach can be applied only to evaluate availability as security attribute with respect to requirement parameters. The validation of, the proposed models are only validated with a small set of data as industry data is unavailable. The recognition of the model is based on perception. However, this approach has been observed in previous research on vulnerability estimation at design phase.

7. Conclusion

Availability is the most significant security requirements. It becomes crucialin real-time systems. The quality of applications such as e-commerce, online banking highly affects by availability of services. Session duration play important role to maintain availability of services. In this paper a model has been developed to quantify availability (MQA^R) from requirement perspective. It estimates the security as availability with respect to requirement parameters which are weighted according to their influence. A multiple linear regression technique is used to quantify the model. The early quantification specifies the quality of software at the early stage of SDLC. Numerical results shown in the work supportsthe claim of acceptability of the proposed model to assess availability that improves the security at the beginning of the software i.e., at requirement phase. The proposed model has been validated and statistical analysis signifies the acceptance of the model.

References

[1] Pfleeger, Shari Lawrence, and Robert K. Cunningham. "Why Measuring Security Is Hard." copublished by the IEEE computer and reliability societies. (2010): 46-54.

[2] Wayne Jansen, "Directions in Security Metrics Research", National Institute of standards and technology, NISTR 7564, March 2009.

[3] M. Grottke, H. Sun, R. Fricks, and K. Trivedi, "Ten fallacies of availability and reliability analysis," in Service Availability, ser. Lecture Notes in Computer Science, T. Nanya, F. Maruyama, A. Pataricza, and M. Malek, Eds. Springer Berlin Heidelberg, 2008, vol. 5017, PP. 187– 206.

[4] Antti Evesti, Eila Niemela, Katia Henttonen and MakoPalviainen, "A Tool Chain for Quality-driven Software Architecting", 2008, IEEE International Software Product LineConference.

[5] DOI: http://www.cert.org.

[6] I. Flechais, M. Sasse and S M V Hailes, "Bringing Security Home: A Process for developing secure and usable systems", NSPW'03, ACM, August 2003, pp: 18-21.

[7] B. B. Madan, K. G. Popstojanova, K. Vaidyanation and K. S. Trivedi, "A Method for Modeling and Quantifying the Security Attributes of Intrusion Tolerant System", An International Journal of Performance Evaluation, 56, 2004, Elsevier. 167-186.

[8] Nikhat, Parveen, Md. Rizwan Beg, et al. "Software Security Issues: Requirement Perspectives." International Journal of Scientific & Engineering Research ISSN 2229-5518. Volume-5.Issue-7, July 2014, pages: 11-15.

[9] G. H. Walton, T. A. Longstaff, R. C. Linder, Computational Evaluation of Software Security Attributes, IEEE, 1997.

[10] DOI: http://www.sqa.net/softwarequalitymetrics.html.

[11] Parveen, Nikhat, Md. Rizwan Beg, and M. H Khan. "Bridging the Gap between Requirement and Security through Secure Requirement Specification Checklist." International Journal of Advanced Computational Engineering and Networking(IJACEN), ISSN: 2320-2106, Volume-3, Issue-2, Feb.-2015.

[12] Iqbal, Shahid, and M. Naeem Ahmed Khan. "Yet another Set of Requirement Metrics for Software Projects."International Journal of Software Engineering and Its Applications. 6.1 (2012): 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): <www.cs.umu.se/education/examina/Rapporter/JaveedAli.pdf>.

[15] C. Wang and Wulf, "A Framework for Security Measurement," in Proc. National Information Systems Security Conference, pp: 522-533, 7-10 Oct. 1997.

[16] S. Chandra, R. A. Khan, "Implementing Availability State Transition Model to Quantify Risk Factor", Advances in Computer Science, Engineering &Application, AISC, Springer, 2012 -, Pages: 937-952.