ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 2, Issue 2, August 2012

Non-Repudiation Related Risk Assessments

S. K. Pandey, K. Mustafa

Abstract- ***At present, security is an essential quality aspect as well as an imperative demand for software projects. A number of approaches, techniques and frameworks have evolved over the time to address security as one of the primary concerns for designing, developing and deploying relatively secure software applications. Security requirements can be used during the software development lifecycle to avoid or eliminate vulnerabilities, particularly during code production, by performing functions such as measuring adherence to secure coding standards, identifying likely vulnerabilities that may exist, and tracking and analyzing security flaws that are eventually discovered. To achieve these objectives, security measures must be embedded throughout the SDLC phases and starting from the requirements phase itself. Non-Repudiation requirement is globally accepted as one of the prominent security requirements. Appropriate level of non-repudiation may well enforce security features and hence, ensure security for deployed software. We have already proposed a checklist in one of our previous papers, which may enable assessment of the appropriateness of non-repudiation requirements. In this paper, by extending our previous work, various attributes of Non-Repudiation are identified and then a weight is assigned to each one, followed by the risk assessment to integrate the steps for security assurance in the SDLC. This will enable the assessment of the aptness of Non-Repudiation in terms of risk and lead to counter/additional measures for security assurance.***

Keywords: **Software Security, Security Assurance, Non-Repudiation, Attributes of Non-Repudiation, Risk Assessment.**

I. INTRODUCTION

In today's technology driven world, accessing information or performing routine tasks such as banking, purchasing goods, booking tickets, paying bills etc. are accomplished through e-portals and web-enabled high end software applications. These activities involve business transactions and also deal with using certain personal as well as confidential information. With the constant appearance of high profile news stories of exposing credit card databases and finding cunning ways into secret systems by hackers, many seriously cautious users do not like to use such services cited security as the major reason, among other risks (Anbalagan & Vouk, 2009). Keeping in mind these incidents, development companies have already acknowledged security as a necessary property to be adapted in all the software; although their security level may vary on case to case basis, depending on relevant parameters. In order to be effective, security must be integrated into the SDLC right from the beginning. Early integration of security in the SDLC enables development companies to maximize RoI (Return on Investment) through their security programs (Assad et al., 2010). This integration enables security to be planned, acquired, built in, and deployed as an integral part of a project or system. It plays a significant role in measuring and enforcing security requirements throughout the phases of the life cycle. Life cycle management helps in the documentation of security-relevant decisions and provides assurance to management that security is adequately considered in all the phases. Early implementation of security in the project in turn facilitates the requirements to be mature as needed and in an integrated and cost-effective manner (Dustin, 2006). One of the most feasible ways to achieve it is the incorporation of security requirements. Security requirements are mainly concerned with 'how assets are to be protected from harm' (Moffett & Nuseibeh, 2003). Security requirements are the constraints on functional requirements intended to reduce the scope of vulnerabilities. Following are the major security requirements traceable in the literature and reported practices (Gilliam et al., 2011):

- Authentication,
- Access Controls and Rights,
- Confidentiality,
- Non-Repudiation,
- Data Classification Procedures,
- Business Continuity and Disaster Recovery,
- Virus Protection,
- Event Log and Audit Trails,
- Backup & Recovery, and
- Incident Management, Intrusion Detection and Forensic Analysis.

In our previous work, mechanisms for the assurance of first three requirements have been covered up to some extent (Mustafa et al., 2008, 2009) (Pandey & Mustafa, 2010). To extend this series one step further, in this paper, we focus on Non-Repudiation. A Non-Repudiation requirement specifies the extent to which a business, application, or component shall prevent a party to one of its interactions (e.g., message, transaction etc.) from denying having participated in all or part of the interaction. A checklist has already been proposed for the verification of major facts related with Non-Repudiation (Pandey & Mustafa, 2011). In this paper, we focus on Non-Repudiation and its related risk assessments. The risk assessment activity is performed on the basis of various attributes identified for this requirement. Beyond this introduction on the background details, remainder of this paper is organized as follows: Section II describes Non-Repudiation. The attributes of Non-Repudiation are discussed in Section III, while a ranking/weight is proposed in Section IV. 'Risk Assessment' is discussed in Section V, whereas 'Experimental Results and Discussion' is given in Section VI. 'Conclusions and Future Work' are given in Section VII.

II. NON-REPUDIATION

Non-Repudiation denotes 'Not denying or reneging'. Digital signatures and certificates offer non-repudiation as they guarantee the authenticity of a document or message (Encyclopedia; and Mccullgh & Caelli, 2000). The basic concept behind this requirement is to provide guidance for the usage of Digital Signatures for electronically signing any document that may need to uphold validity for the purpose of non-repudiation, as a manual signature or thumb impression on a physical document, in the court of law, as per the applicable Act, e.g. Information Technology Act (Amended), 2008 in India. All the legal documents, in electronic format should be signed using Digital Signatures. Any other electronic document that may require validity and non-repudiation in the court of law should be signed using Digital Signature. The Digital Certificate, which is used for digitally signing any such documents, will be treated as a valid certificate in any court of law, issued by a 'Licensed Certifying Authority'.

III. ATTRIBUTES OF NON-REPUDIATION

Taking into account, the need and significance of Non-Repudiation for building secure software, various attributes of this requirement attributes have been derived from the reported and well-verified practices, which is evident from our earlier publication (Pandey & Mustafa, 2011). A pictorial representation of these attributes is depicted as follows:

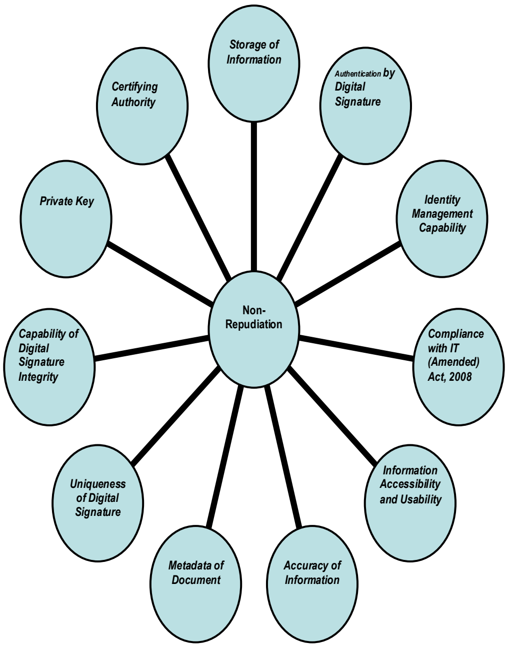
Storage of Information
Certifying Authority
Authentication by Digital Signature
Private Key
Identity Management Capability
Non-Repudiation
Capability of Digital Signature Integrity
Compliance with IT (Amended) Act, 2008
Uniqueness of Digital Signature
Information Accessibility and Usability
Metadata of Document
Accuracy of Information

Fig. 1: Attributes of Non-Repudiation

IV. RANKING/WEIGHT OF THE ATTRIBUTES

After proposing these attributes, we realized that each attribute may have its unique weight for the implementation of this security requirement; that means the ranking/weight of all the attributes may not be the same rather it will be different. Therefore, it was decided to take the help and guidance of experts' feedback by designing a feedback form. The feedback was collected on the following issues:

- Analysis of the attributes' quality which include following heads:
  - Importance of the attribute,
  - Potential utility for evaluation practice,
  - Completeness/coverage of attributes, and
  - Relevance of all the attributes, and
- In the rightmost column of each attribute, to assign a *weight between 1 and 5 (1 is minimum and 5 is maximum)* to each attribute for the implementation of this security requirement.

These attributes along with the review form were sent to the thirty experts from the varied fields' viz. academia, industry, scientific organizations, educational institutions, research bodies, government organizations. Really, it was a daunting task to have the feedback from the experts. After a long exercise, we were able to have duly filled feedback forms from the twenty experts only. After collecting these forms/comments, we compiled this data in two ways. At the first level, based on the comments cited in the review forms, we made some revisions in the attributes and then again a fresh ranking was taken. On the second level, we designed a format in an excel sheet, in which all the data from the experts' comments were filled. Since, we received the feedback from twenty experts only; an average value for each attribute was calculated. Based on the average value of each attribute, we finalized the weight of the attributes of Non-Repudiation, which is displayed in the following table:

Table.1: Attributes' Weight of Non-Repudiation

S. No.	Attribute	Attribute's Weight
1.	Storage of Information	4.80
2.	Authentication by Digital Signature	4.50
3.	Identity Management Capability	4.75
4.	Compliance with IT (Amended) Act, 2008	4.70
5.	Information Accessibility and Usability	4.40
6.	Accuracy of Information	4.65
7.	Metadata of Document	4.60
8.	Uniqueness of Digital Signature	4.25
9.	Capability of Digital Signature Integrity	4.45
10.	Private Key	4.45
11.	Certifying Authority	4.40

V. RISK ASSESSMENT

After determining the weight of the attributes of the Non-Repudiation, we hereby propose the risk assessment procedure, which can be done by using the following formula:

Compliance Factor of Non-Repudiation,
$CF_{N\text{-}R} = \sum W_i X_i \,/\, n$ where $X_i = \{1$ or 0

$i = 1, 2, 3, \ldots\ldots\ldots\ldots n$

Here, W_i is the weight of the attribute, and X_i is the value based on the compliance/non-compliance of this attribute i.e. if a attribute is compliant, the value will be 1, and if not, its value will be 0.

Based on the value of CF_{N-R}, its tolerance limit may be decided. However, we propose the following limits:

- **Low Risk:** The implementation of this requirement is at low risk if the value of the CF_{N-R} is ≥ 3.5.
- **Medium Risk:** The implementation of this requirement is at medium risk if the value of the CF_{N-R} lies between 2.5 to 3.5.
- **High Risk:** The implementation of this requirement is at high risk if the value of CF_{N-R} is $\leq$ 2.5.

VI. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed methodology is applied to a real life project of a software development company (on the request of the company, identity is concealed), and the final result of attributes' assessment is calculated on the bases of the compliance status. The results are given in the following table:

Table 2: Tryout Data for Non-Repudiation

S. No.	Attribute	Attribute's Weight (W)	Compliance Status (X)	Weighted Compliance Factor (WCF)
1.	Storage of Information	4.80	0	0
2.	Authentication by Digital Signature	4.50	0	0
3.	Identity Management Capability	4.75	1	4.75
4.	Compliance with IT (Amended) Act, 2008	4.70	0	0
5.	Information Accessibility and Usability	4.40	0	0
6.	Accuracy of Information	4.65	0	0
7.	Metadata of Document	4.60	1	4.60
8.	Uniqueness of Digital Signature	4.25	0	0
9.	Capability of Digital Signature Integrity	4.45	0	0
10.	Private Key	4.45	0	0
11.	Certifying Authority	4.40	0	0
				∑ WCF = 9.35
CF_{N-R} = **(9.35) / 11= 0.85**				

Now, the value of the CF_{N-R} is compared with the threshold values, as specified above. However, it can also be decided by the requirement engineers according to the security needs; the threshold value may vary according to the security requirements of the software. Here, the value of the PCF is 0.85, which is at the high risk. This value is not tolerable at any cost. Hence, requirement engineers should revise the SRS by strengthening the Non-Repudiation requirements. For the comparison of results, we demanded the results from the development company after using their existing tools/techniques for the same. But, they were unable to provide any quantified value; they could only provide a general opinion as saying that 'we rate the SRS highly insecure with reference to the Non-Repudiation requirements'. Their qualitative revelation about the final results confirms our quantitative results. From these evidences, the utility of our proposal is automatically ascertained up to some extent. However, it may not be as much as necessary to conclude so strongly about the effectiveness of the proposal but certainly, up to some extent.

VII. CONCLUSION AND FUTURE WORK

The attributes of Non-Repudiation are identified and a weight has been proposed for the implementation of the same. A risk assessment formula is also proposed for determining the risk related with this requirement. The system will be stronger with respect to this requirement if it satisfies all or most of the attributes and will be on the low level of risk. A complete process of Non-Repudiation requirements is described for the security assurance of the SRS. Being prescriptive in nature, the proposal may be useful towards implementing security *'right from the inception itself'*. Moreover, these proposals need to be validated in large samples for standardization. Therefore, future work may include the integrated level validation of the proposal along with the standardization for a large sample space. A software tool may also be developed for the automation of this complete process. In future, we are also trying to identify the attributes of other remaining security requirements given in the section I, based on the same pattern. The proposal may help software developers and security experts for building secure software.

REFERENCES

[1] Anbalagan, P. & Vouk, M. (2009). Towards a Unifying Approach in Understanding Security Problems. International Symposium on Software Reliability Engineering, (pp. 136-145). Mysuru, India.

[2] Assad, R. E., Katter, T. and Ferraz, F. S. (2010). Security Quality Assurance on Web-based Application Through Security Requirements Tests. In proceedings of Fifth International Conference on Software Engineering Advances, (pp. 272-277).

[3] Dustin, E. (2006, June). The Secure Software Development Lifecycle. Retrieved June 12, 2008, from http://www.devsource.com/c/a/techniques/The-Secure-Software- Development-Lifecycle/

[4] Encyclopedia. Non-repudiation. PC Magazine Encyclopedia. Retrieved March 2, 2010 from http://www.pcmag.com/encyclopedia_term/0,2542,t=nonrepudiation&i =48067,00.asp

[5] Gilliam David P., Kelly John C., Powell John D., Bishop Matt. (2011). Development of a Software Security Assessment Instrument to Reduce Software Security Risk. In the Proceedings of the WETICE (pp. 144-149).

[6] Mccullgh Adrian & Caelli William. (2000, August 7). Non repudiation in the digital environment. First Monday, 5(8). Retrieved May 3, 2008 from http://www.firstmonday.org/issues/issue5_8/mccullagh/

[7] Moffett, J. D., & Nuseibeh, B. (2003, August). A Framework for Security Requirements Engineering. Department of Computer Science, YCS368. University of York UK.

[8] Mustafa K., Pandey S. K., Rehman S. (2008, September). Security assurance by efficient access control and rights. CSI Communication, 32(6), 29-33.

[9] Mustafa K., Rehman S., Pandey S. K. (2009, March): Confidentiality related security assessments. IEEE International Advance Computing Conference. Patiala.

[10] Pandey S. K., Mustafa K. (2011, December). Security assurance by efficient non-repudiation requirements. International Conference on Communication Security and Information Assurance, New Delhi, India. (communicated)

[11] Pandey S. K. & Mustafa K. (2010, July-Aug). Security Assurance: An Authentication Initiative by Checklist. International Journal of Advanced Research in Computer Science. 1(2), 110-113.