Name of the Research Scholar : Santosh Kumar Pandey
Name of the Supervisor : Prof. K. Mustafa
Name of the Department : Computer Science
Title of the thesis : Security Risk Assessment through SRS

ABSTRACT

The evolution of internet has brought a radical change in the sphere of learning and knowledge sharing. This interconnectivity and accessibility has proved its worth. There are various advantages of such high speed connectivity and grouping of networks but it is rightly said that *'excess is always bad'*. So, case is the same here as along with certain advantages, there are some drawbacks too. The risk of malicious attacks to the software security considerably has gone up and to prevent such risk is very necessary. It is the prime concern for the software engineers and researchers to address this burning issue. The identification of risk is not an easy task as it requires a thorough understanding and keen eyes for observations. It also requires sincere efforts to pursue research in this context. It is very necessary to adapt and apply the measures to assess and prevent the risk.

The maxim *'sooner is better'* has become the order of the day. Hence, this study is undertaken in view of the significance of risk assessment in the requirements phase of SDLC. In the first instance, it is considered imperative, in the absence of any roadmap/process/framework, to propose a framework for the risk assessment through SRS. Subsequently, a review of literature on the major available risk assessment methodologies is undertaken. By establishing a comparative study, it is revealed that the available methodologies do not fulfill the needs and there is an ample scope for evolving a new methodology/framework. For the development of the said framework, it is realized that there must be security policies' checklists and attributes along with their respective weightage.

The current research has three major areas, our proposal: RAF, validation data, and interpretation of results. The first component is the development of *nine security policies checklists* on the basis of the review of literature, particularly the number of industry best practices for the implementation of each security policy. The second component is the *determination of various*

attributes and their individual weightage for each security policy. In the third major component, *Risk Assessment Framework (RAF)* has been proposed. The proposed framework, for the risk assessment in requirements phase has been validated by using RAF tryout on five SRSs of live projects. The results obtained by using RAF are also compared with the final results/recommendations of the industry and these are found to be highly similar to the results obtained by using RAF. Apart from these components, some of the primary research questions for the study are also addressed during the course of study.

Such type of studies is evolving in nature. Therefore, a number of typical extensions/modifications may be inevitable, in view of the fast growth in the ICT applications. The proposed framework along with the checklists of major security policies can be effectively used in assessing the risk for the requirements phase. A software tool may also be developed for the automation of the complete process. In future, depending upon the need of the project and advancement in technology, some more policies may also be added. This work may also be extended for the further phases of SDLC by developing various checklists as per the requirements. Like any other study, the work has its own limitations and delimitations. Therefore, in order to generalize the results, study can be done by organizing and analyzing a large sample of SRS, in future.