Notification No: F.NO COE/Ph.D./(Notification)/526/2022

Date of Award:30/12/2022

Name of the Scholar: Aditya Dev Mishra

Name of the Supervisor: Prof. (Dr.) Khurram Mustafa

Name of the Department: Department of Computer Science

Name of the Centre: Faculty of Natural Sciences

Topic of Research: Security Requirement specification by formal methods

Finding

In the last few years, the field of software security requirement has changed radically. Security requirement specification is now one of the most widely recognized, actively pursued challenges in both the software engineering and information assurance communities. A majority, almost 50%, security problems originate in this phase and culminate into inadequate/inaccurate specifications; lead to huge fixing-efforts and cost enormously. Therefore, there is a need to specify the security requirement more precisely, consistent, and adequate. Many software security problems originate in the inadequate or inaccurate specification of the requirements for the software or from the mismatch between the interpretations of the requirements during development and their actual intent. Formal methods are a mathematical approach for specification, development, and verification of software product. Formal methods can be used to precisely specify requirements such that one can later prove an implementation meets those requirements. Formal methods act as evidence which ensures that the system indeed satisfies the demand of security, reliability, and correctness.

Considering the need and significance of formal specification and security requirement specification, a study on security requirement specification by formal method was proposed. The approach includes identification, classification, and analysis of requirements specification at security level and development of formal methods framework. That is, it was proposed to

evolve a prescriptive framework that enables a security expert to scan through security requirement specification, identify the security requirement and specify by formal methods. Thereby, a generic framework for security requirement specification by formal methods has been proposed. The objective of the proposed framework is the integration of security in requirement engineering with a formal approach. Thus, the proposed framework is to assist security engineers about classification, analysis, and specification of security requirements through a formal method in a more systematic way during the requirement engineering process.

The framework SRSFM may be also used to transform the ambiguous security requirements, if any, into formal by following the prescribed steps and guidelines. The proposed framework was pre-validated by expert review and some of their suggestions were taken care of by corrections/modifications. It was validation by implementing a case study of mobile banking application. Moreover, the post validation was accomplished by using the Z word and alloy model checker tool based formal verification and validation of security properties. In this way, the effort to develop a prescriptive, user friendly, generic framework seems valuable for software development and a substantial contribution to the field of security requirements specification using formal methods.