Notification No.: F.NO. COE/ Ph.D./(Notification)/517/2022
Date of Award: 13-07-2022

Name of the Scholar : **Malik Nadeem Anwar Mohammad**
Name of the Supervisor : **Prof. Mohammed Nazir**
Name of the Department/Centre : **Computer Science**
Topic of Research : **Modeling Security Threats during Requirements Elicitation**

Keywords

Security threats, Requirements Engineering, Modeling threats, Formal modeling, Petri Nets, Security Requirements Engineering.

Abstract

Software systems in today's world have become an indispensable part of human life. The advancements in software applications has led to the unprecedented developments in the field of education, health, finance, transportation, industries, telecommunications, and defense. Majority of the software applications are being used in the prevailing distributed computing environment and are continuously being tracked by the attackers for their ill intentions. Consequently, modern society has become a soft target for the sophisticated security attacks. Modern systems face security and privacy threats as a result of the plethora of interconnected services, components, and technology. Vulnerabilities and threats in any part of the interconnected system may cascade and zoom out over the entire system. Researches unanimously agree that most of these attacks are attributed to poor threat modeling practices during the requirements phase of SDLC. The risk of security attacks and the cost of fixing them continue to grow exponentially. In fact, it has been widely acknowledged that the cost for fixing the defects reduces significantly when they are addressed at the requirements phase. Threat modeling during the requirements phase can help in detecting early flaws and threats in the system. It provides an opportunity to revisit and refine the architectural defects and security requirements of the system. Unlike traditional software testing techniques like penetration testing and fuzz testing, threat modeling at the requirements stages ensures a proactive approach, where the vulnerabilities and the anticipated threats are detected and rectified well in advance, before it creeps into the system. Recognizing the importance and necessity of threat modelling during the requirements elicitation phase, this thesis focuses on building effective frameworks, models, and formal techniques for effectively modelling threats during the requirements elicitation phase. A review of the literature indicated that systematic and well-defined threat modeling approaches which consider important constructs like assets, vulnerabilities, and risk,

which are essentially needed to model threats, are missing in the current approaches.

The study has followed a systematic methodology to carry out the research work. First, a Systematic Literature Review of the relevant literature on ‘Security Requirements Engineering' (SRE) is conducted in accordance with Kitchenham's guidelines. The methodology involved a multi-stage rigorous filtering process and 108 papers were selected from the literature. These papers were critically analyzed to outline 20 different SRE approaches. The SRE approaches were analytically evaluated and compared based on relevant criteria like usability, publication frequency and trends, support in different sub-phases of the requirements phase and terminologies adopted. The SLR helped us to find the research gaps, critical findings, and recent developments in the domain of SRE.

To address some of the research gaps identified in the Systematic Literature Review (SLR), we proposed the MUCX model, an extended version of the well-known UML-based Misuse Case model. MUCX visualizes all the possible threats and their effects, along with possible vulnerabilities, and assets affected. Threats and vulnerabilities capture the likelihood of occurrence of the threat, while the harm caused to the assets and their severity determines the possible consequences. The risk spots in the MUCX diagram captures the combined effect of threats and vulnerabilities on the assets. We successfully validated the MUCX model on an e-voting system and identified several potential threats, vulnerabilities, and risk spots, thereby producing phase-wise MUCX diagrams.

A Framework for formalizing the misuse case model using High-Level Petri Nets has been developed. The framework converts the misuse case diagram to a level 1 Petri Net, refines each of the activities in the misuse case diagram to create level 2 Petri Nets, and finally substitutes them in the main net to create a Hierarchical High-Level Petri Net model. The substitution process is backed by a rigorous mathematical treatment to assure various properties like safeness, boundedness, and liveness of the formalized model. The framework was validated by modeling, simulation, and analysis of a simple ATM system using the CPN tool.

A systematic evaluation and improvement of notations in the MUCX diagram, have been performed, based on the “Physics of Notation” (PoN) principles. Several issues like symbol overload, symbol excess, and lack of visual expressiveness were highlighted in the existing notations. The proposed changes were done for improving various properties like perceptual discriminability, visual distance, semiotic clarity, and visual expressiveness. The improvements suggested in the existing notations were validated using a survey-based empirical study involving students and subject experts. The survey results largely indicate that the respondents find the new notations more appealing and descriptive. The results also highlighted that the new notations are semantically more transparent as compared to the original notations.