Name : Shabana Rehman

Supervisor : Prof.K.Mustafa

Department : Computer Science

Title : OOD Security Vulnerabilities and Mitigation Mechanism

ABSTRACT

Attack on hardware of information system is quite difficult, as attacker needs a physical access and lots of critical information about the system. However, attack on software of information system is far simpler then the hardware, the attacker just need an information about *one vulnerability in the software* and can exploit vulnerability remotely without leaving any trace. Minimizing a number of security vulnerabilities in software is one of the most urgent needs in the computer security today and design is the most important phase were vulnerability mitigation gives a substantial benefit to the developer. According to Computer Emergency Response Team, USA, more than 90% of vulnerabilities leak out during system development. They are the result of ignoring known vulnerabilities found in other systems. Known vulnerabilities can be used to help vaccinate the security process that can avoid vulnerabilities in the new software. The mitigation mechanisms of all most all the known vulnerabilities are available but designers do not use them due to the lack of organized information and limited time for developing software.

Keeping in view the importance of software design level security vulnerabilities, a study of current software design level security vulnerabilities is conducted and software design level 'OOD Security Vulnerabilities and Mitigation Framework' is proposed. It consists of three main components including (i) A Taxonomy of design level vulnerabilities, (ii) A Classification Model and (iii) Security Requirement Risk Mitigation process. The Taxonomy is developed to organize security related vulnerability information under specific classes of vulnerabilities. This taxonomy can be used to understand and mitigate vulnerabilities on the cluster basis and thus eliminate the need of individual analysis of each of the vulnerabilities. NVD (National Vulnerability Database) database is used for the analysis of vulnerabilities. Taxonomic features were identified after analysis of vulnerabilities using priori classification. Average severity of each class of vulnerability was calculated using CVSS (Common

Vulnerability Scoring System) equations, which was further used to identify weightage of each class of taxonomy. After the development of taxonomy, a classification model was developed using machine learning techniques. SVM (Support Vector Machine) was used as the classification technique and bootstrap validation is used to validate the final classification model. The model was designed using Rapidminer tool. The classification model will indicate the developer on vulnerability mitigation. If vulnerability is identified as a design level vulnerability then it will indicate the security feature class it falls into. After knowing the class of security feature, designer would need processes that can prevent these vulnerabilities. To deal with this issue, we have developed a list of authentic and reliable database of available security design patterns. These patterns can be used by the designer to prevent these vulnerabilities. An analysis is also performed on the identified design patterns, and all the patterns are classified into three levels. After identifying the vulnerabilities, the designer can choose the level of the design pattern according to the severity of the vulnerabilities.

In order to mitigate the vulnerabilities from the requirements of the software, a security requirement risk mitigation process was developed. In this process, 'Common Criteria Standard' is used to measure the strength of security requirements. If a developer wants to prevent vulnerabilities right from the requirement phase of SDLC then he can simply choose the security requirements from a set of common criteria security requirements, then these security requirements are measured in terms of security feature class that we have used in the vulnerability taxonomy development. On the basis of these security feature class value, adequate mitigation measures in the form of design patterns are proposed, that can be used by the software designer to create relatively secure software. A combination of 'Classification Model' and 'Security Requirement Risk Mitigation Process, forms a framework entitled *OOD Security Vulnerability Mitigation Framework*, Tryouts and Validation was carried on eight live projects in the industry. The Results after validation of the framework are found to be promising and indicate the importance of the work.