Assessing the Impact of Re-engineering on Software Security

Introduction

In today's technology-driven world, software is ubiquitous, and security is a primary concern for software developers, users, and organizations. Software reengineering, the process of modifying and improving existing software, is often necessary to keep up with changing technologies, user needs, and business requirements. However, reengineering can also introduce new security vulnerabilities, which can have severe consequences for software systems and their users. This project aims to assess the impact of software reengineering on security and survey best practices and guidelines for mitigating security risks during the reengineering process.

Background and Motivation

Software systems are vulnerable to various security threats, including malware, viruses, hacking, and cyberattacks. These threats can cause significant damage to software systems, result in data breaches, and compromise user privacy and security. Therefore, it is essential to ensure that software systems are secure and resilient to potential security threats.

Software reengineering is an essential process for maintaining and improving the quality and functionality of software systems. However, the process of reengineering can also introduce new security vulnerabilities that can compromise the security of software systems. For example, software reengineering may involve modifying and restructuring the software code, which can result in the introduction of new security vulnerabilities that were not present in the original code. Therefore, it is essential to assess the impact of software reengineering on security and survey best practices and guidelines for mitigating security risks during the reengineering process.

Objectives and Scope

The primary objective of this research paper is to assess the impact of software reengineering on security and survey best practices and guidelines for mitigating security risks during the reengineering process. To achieve this objective, we will conduct a comprehensive analysis of relevant literature on software reengineering, security risks, and mitigation strategies. We will also analyze case studies of software reengineering projects to identify the security risks and impacts of reengineering on security. To provide recommendations for practitioners and researchers for ensuring software security during the reengineering process

The scope of this research paper includes assessing the impact of software reengineering on security, identifying the security risks associated with software reengineering, and developing best practices and guidelines for mitigating security risks during the reengineering process. We will focus on various reengineering techniques and their impact on software security.

Methodology

To achieve the objectives of this research paper, we will adopt the following methodology:

Literature Review

A comprehensive review of relevant literature on software reengineering, security risks, and mitigation strategies will be conducted. The literature review will provide insights into the impact of reengineering on security and identify best practices and guidelines for mitigating security risks during the reengineering process.

Case Studies

Case studies of software reengineering projects will be analyzed to identify the security risks and impacts of reengineering on security. The case studies will provide insights into the real-world impact of reengineering on security and help identify best practices and guidelines for mitigating security risks during the reengineering process.

Analysis and Validation

The results of the literature review, case studies, and experiments will be analyzed and validated to survey best practices and guidelines for mitigating security risks during software reengineering. The analysis and validation will involve identifying the security risks associated with software reengineering and developing best practices and guidelines for mitigating these risks.

Expected Outcomes

The expected outcomes of this research paper include: A better understanding of how re-engineering affects the security of the system. Judge better on how well the security of a modernized system works.