Security in Software Engineering

Swetha Paka
Spaka1@student.gsu.edu
Panther ID: 002268388

Raghunandan Gardas
Rgardas1@student.gsu.edu
Panther ID: 002302325

Abstract

Security has emerged as one of the most significant challenges to organizations that develop software systems. Software today is critical in every domain of society and business and it is paramount that this software be secure. Most software systems involve managing financial systems, infrastructure and industrial systems. The consequences of unauthorized access to those systems compromises both the data and the system of the industry. Traditionally, the disciplines of software engineering and security engineering have worked in separate silos which has given a chance for vulnerabilities and bugs to arise in a software.

To have high assurance and reliability for any software it is important to embed security requirements into the SDLC (Software Development Life Cycle). Embedding Software and Security Requirements together results in a bug free software for the user. As in traditional SDLC, security testing is done at the end but it should consider security and risk factors at every stage of software development to prevent major bugs at the later stages.

We discuss the importance of security in software engineering and methods to merge traditional SDLC with risk and security properties into one life cycle and discuss further research in Secure Software Engineering. Similar to functionality testing it is equally important to integrate software testing during the Testing phase of a Software. It also discusses about an integrated security testing framework for Secure Software Development Life Cycle.

The review will help the class understand the role of security in software development. It also gives the class an idea of the challenges that exist in embedding security requirements into a software. It also gives them knowledge about how to integrate security and perform security testing for a software systems.

Main References


Other References: