Al-Quds University

Deanship of Graduate Studies

Improving Software Security in Software Life Cycle Models

Ahmad Jamel Fahel

M.Sc. Thesis

Jerusalem – Palestine

1430 / 2010

Al-Quds University

Deanship of Graduate Studies

Computer Science Department

Improving Software Security in Software Life Cycle Models

Prepared By:

Ahmad Jamel Fahel

Supervisor:

Dr. Raid AL-Zaghal

Thesis Submitted in Partial fulfillment of requirements for the Master

Degree of Computer Science from Computer Science department of Al-Quds University

Jerusalem – Palestine

1430 / 2010

Al-Quds University

Deanship of Graduate Studies

Computer Science Department

Thesis Approval

Improving Software Security in Software Life Cycle Models

Prepared By: Ahmad Jamel Fahel
Registration No: 20714277

Supervisor: Dr. Raid AL Zaghal

Master thesis submitted and accepted. Date: 23/6/2010

The names and signatures of the examining committee members are as follows:

1- Head of Committee: Dr. Raid al-Zaghal	Signature: ……..
2- Internal Examiner: Dr. Nidal Kafri	Signature: ……..
3- External Examiner: Dr. Osama Marie	Signature: ……..….

Jerusalem – Palestine
1430 / 2010

Declaration

I certify that this thesis submitted for the degree of master of computer science is the result of my own research, except where otherwise acknowledged, and that this thesis (or any part of it) has not been submitted for a higher degree to any other university or institution.

Signature:

Ahmad Jamel Fahel

Acknowledgments

Praises and thanks always are to Allah, The creator, and the teacher.

Then, I would like first of all to state my thanks to my supervisor Dr. Raid Al-Zaghal for his great support, effort and advice during my study period and especially the course of my thesis.

Also, I am grateful to all teachers at Al-Quds University/Computer Science Department. This thesis would not have been possible unless their encouragement.

Our thanks are also extended to doctor Nidal Kafri, Dr. Osama Amin and all our academic staff.

And thanks to my mother, brothers and sisters. I will never forget the support and encouragement from my wife; my great thanks to them for their love and inspiration.

Dedication

To my parents, wife, brothers and sister

To all Alquds University friends and colleagues

To all postgraduate students at Al-Quds University

To all those who help me during my study

Abstract

Software security is a major issue in software engineering, and the principles of software security are very clear to understand, but they are usually hard to implement. This is due to many security vulnerabilities that deter achieving a high level of security in software systems.

In this thesis, I have collected information on relevant security vulnerabilities; I described and classified them into levels according to their risk degrees. To do that, I have built a model based on different stages: (1) a learning stage to give the system engineer full and clear information about these security vulnerabilities, (2) a prediction stage that depends on the collected information to predict the possibility of each vulnerability and its effect (harm level) on the system, (3) in the scenario stage, the system engineer writes one or more scenarios to describe the circumstances (how and where) that would lead for each vulnerability and then suggests a preventive plan to avoid that vulnerability, (4) in the testing stage, the software is tested with all predictions on spot by running a fuzzy test to be sure that the software is secure against known vulnerabilities, (5) and in the final stage, I write the implementation for the system auditor to check the overall security level of the software.

We have suggested a plan to integrate this model into the four common phases of the software development lifecycle.

ملخص الرسالة

تعد حماية البرامج من الثغرات من اهم الامور التي تناقش مرارا وتكرارا نتيجة ظهور أنواع متعددة من الثغرات, ويعد العمل على حماية البرامج من الامور الصعبة في بعض الميادين لان بعض البرامج تتعرض لثغرات نتيجة لغة البرمجة المستخدم والبيئة اللتي يستخدم بها البرنامج , اضافة الى الفهم الصحيح للثغرات الامنية اللتي لا تطرح عادة ضمن مراحل حياة البرنامج على اختلاف انواعها.

إبتدأت في هذه الرسالة بجمع الثغرات الامنية وجميع المعلومات عنها من مصادر مختلفة , و قمت بتصنيف هذه الثغرات بحسب اهميتها ونوع لغات البرمجة اللتي تستطيع هذه الثغرة اختراقها او الانظمة المستضيفة للبرامج وكيفية الوقاية من الثغرات او تجنب حدوثها.

وبعد دراسة مستفيضة للثغرات الامنية قمت ببناء نموذج مبسط لتسهيل تجنب الثغرات الامنية ولتعليم المستخدم لهذه النموذج الثغرات الامنية التي قد تواجهه اثناء تطويره نظام معين ويتكون هذا النموذج من المراحل التالية :

1- التعلم : يتم من خلاله المرور على جميع الثغرات الامنية ودراستها جيدا
2- التوقع : يتم جمع جميع الثغرات الامنية المتوقع حدوثها بناءً على معطيات البرنامج المنوي عمله
3- كتابة طريقة تجنب حدوث الثغرة
4- تطبيق الطريقة المكتوبة في الفقرة السابقة
5- فحص البرنامج بناءً على التوقعات المحتملة
6- كتابة تقرير بالثغرات اللتي تم التنبه لها

وبعد ان قمت ببناء النموذج اقترحت الية دمجه مع آليات تطوير البرامج المستخدمة من قبل المطورين , والية فحص البرنامج من ناحية امان البرنامج , والية قياس النموذج المقترح بناء على المراحل اللتي يتم بها تطوير البرنامج.

Structure of Thesis

This research contains six chapters: the first chapter presents an introduction on software security and gives a short problem description, the second chapter gives a background on software security and illustrates relevant definitions and concepts, the third chapter discusses related works and other modules on the security lifecycles, the forth chapter presents our model and how to test software security and test security models, and also contains data on how to integrate our model with other software lifecycles models. The fifth chapter presents a real case on how to use this model with web applications, and the sixth chapter presents future work.

Table of Contents

List of Tables

List of Figures