Report Outline for Whether Security Problems Always Be Publicly Disclosed (Con)

The Issues and Frequency of Security Problems

What are the common issues we face regarding security and how frequent are they?

Overview of the Solution

How public repositories can help us regarding security problems.

How we can use public repositories to help us address security problems

How we can develop a state-based process model of the security problem to address it

In what way(s) can a state-based process model help us address security problems? What is its role? What are our expectations from it?

How developing security sub-models will help us address this problem

What are the security sub-models that we will need? How many are they? How are they developed? What is each one's intended role? What do we expect from each one of them?

Empirical Analysis

What is empirical analysis?

How do we get the data that will be analyzed?

What are our sources to get the data that we intend to analyze?

How to use the collected data properly for analysis

How to analyze the collected data?

Security Problem Response Model

Introduction

What is the security problem response model?

How the response model is created

How do we create a security problem response model

Example of Security problems from an open-source database

Case study and its results.

Predictive Modeling

What is predictive modeling?

What is the Classical Software Reliability Model on Security Data

What is the Classical Software Reliability Model? How reliable is it when it comes to security data?

Bayesian Model

What is Bayesian Model

How we can model Disclosure related belief

Evaluation of the Bayesian Model

Operational use of the Bayesian model

Disclosure and Patching Policies Analysis

Impact of Security Failures

What are the effects of security failures?

Impact of Patching Policies

What are the effects of patching policies?

Why Security Problems Should Not Always Be Publicly Disclosed

Conclusion