Applying dynamic taint propagation in order to enforce domain driven security

Specification and Time Schedule

FREDRIK ADOLFSSON

Master in Computer Science
Date: January 26, 2018
Supervisor: Musard Balliu
Examiner: Mads Dam
Swedish title: Tillämpa dynamic taint propagation för att genomdriva domändriven säkerhet
School of Computer Science and Communication

Contents

Chapter 1

Background

Domain Driven Security (DDS) is a methodology that can be seen as a extension to Domain Driven Design (DDD). The core concept is about the the focus on the development of the domain models and making sure that they are correctly described and built so validation before propagation can be correctly executed.

The thesis is of importance in the security field where avery step towards more secure software is something good. However, the work will gain those who practices the methodology of DDS.

1.1 Objective

The concept of DDS have been born and in development from consultants at Omegapoint. That means that everything that might validate, invalidate or evolve the mythology in any way is of interest for them. The topic for the given thesis was born and discussed at their latest internal conference. Since Omegapoint regularly offers thesis positions was this a excellent topic to offer. Except for a thesis that is of KTH's expected standard do they have a interest in seeing a prototype of a possible implementation of a dynamic taint propagation tool to support practitioners of DDS. Not ready for production but as a test to see if it could be a possibility.

Chapter 2

Research Question & Method

How can dynamic taint propagation help a practitioner of Domain Driven Security.

2.1 Problem Definition

The challenge is to implement a

2.2 Examination Method

2.3 Expected Scientific Results

Chapter 3

Evaluation & News Value

3.1 Evaluation

3.2 Work's Innovation/News Value

Chapter 4

Pre-study

Chapter 5

Conditions & Schedule

5.1 Resources

5.2 Limitations

5.3 Company Supervisor

5.4 Schedule