Applying dynamic taint propagation in order to enforce domain driven security

Specification and Time Schedule

FREDRIK ADOLFSSON

Master in Computer Science
Date: January 29, 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 focus on the development of the core 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 first challenge is to implement the dynamic taint propagation tool. It should be sufficient for it to be a prototype and not a tool that is ready for deployment. The second challenge will be to evaluation how well the tool might help a DDS practitioner. It might be possible that it is not worth using at all because of possible overhead it might entail.

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

The literature study will focus on taint propagation and domain driven design/security and what they are all about. Research into JVM modifications must also be included since it is needed for the implementation of the dynamic taint propagation tool. The information will be obtained by researching for relevant books, reports and other relevant material. Two of the founders of the concept of Domain Driven Security work at Omegapoint and are accessible for questions.

Chapter 5

Conditions & Schedule

5.1 Resources

No special equipment is needed for the project. But depending on the direction of the thesis might a, or more, already existing program implemented on the JVM be needed. They can be used to evaluate the dynamic taint propagation tool to see if we can find vulnerabilities in them.

5.2 Limitations

The dynamic taint propagation shall not be a production ready tool. It should be a proof of concept.

5.3 Company Supervisor

- **Simon Tardell:** Is my supervisor in the technical parts of the thesis. He's also constructed a first draft of the dynamic taint propagation tool which I am free to use.
- **Jonatan Landsberg:** Will assist with supervision on the academic part if the thesis.

5.4 Time Plan

Below is my time plan for the Masters Thesis. The goal is to continuously, trough out all the phases, add to the report. But I've also reserved a couple of weeks in the end for writing the report. I believe that this time can be used to polish the report and rewrite sections if needed.