Exjobb specification

Suggested title: *Test-oriented runtime verification - Using a test-like specification syntax for runtime verification.*

Adam Renberg, 19880429-6211, 070-165 34 69, adamre@kth.se

June 5, 2012

Institute/School:	School of Computer Science and Communication (CSC) at KTH
Company	Valtech

Supervisor, Valtech:	Erland Ranvinge	erland.ranvinge@valtech.se
Supervisor, KTH:	Narges Khakpour	khakpour@liacs.nl
Examiner, KTH:	???	???
Coordinator, KTH:	Ann Bengtsson	ann@csc.kth.se

Website:	http://tgwizard.github.com/thesis/
Repository:	http://github.com/tgwizard/thesis/

The suggested topic is runtime verification (RV) of [web] systems. As suggested by both Erland and Narges, this is of great interest in both the industry and the academic community. The exjobb will be done at Valtech.

RV is a light-weight formal verification technique that is embedded in systems. It verifies that certain properties hold at certain points in the code *during execution*. These properties are specified in a constructed language, often a logic/calculus, and an RV framework instruments the system to be monitored with code that verifies these properties. When a property violation occurs, simple actions can be taken (e.g. log the error, send emails), or more complex responses initiated, resulting in a self-healing system.

The specification languages used by RV implementations is often based on some formal logic and not written in the main language. In contrast, offline unit testing frameworks, such as *JUnit* for Java or *unittest* for python, often utilize the main language to great effect,and their use is wide spread.

This exjobb will be an investigation into RV, how it is used today, and how an RV framework could be implemented with inspiration from offline unit testing frameworks. The idea is to find an RV specification syntax that closely resembles that of offline unit testing frameworks, thus making RV fit better into existing software development (processes), where unit testing is ubiquitous and well accepted.

An important part of RV specifications is that they should be formal, and thus that the properties they specify yield a formal proof of correctness for the current execution. With a more lenient syntax for the specification language, such as a fully fledged programming language, we need to ensure that the formal properties still hold.

We need to:

1. Define the syntax for the unit test-like RV specification
2. and relate this to a formal logic, to ensure the correctness of the specification
3. and instrument the code to monitor the system and build the system model
4. which will be used (online) to verify the system against the specification

We will focus on item 1 and 3.

The exjobb will be split in these parts:

- Background and state-of-the-art "inventory". What is RV? Why does it exist? Research results? How is it applied in practice? How is it used in web contexts? How are specification languages chosen and designed?
- Background and state-of-the-art of testing frameworks and their languages/syntax.
- Investigation of how RV can be applied to a (web) system. What specification language to use? In what system language: dynamic (python, ruby, etc.) static (Java, C#)? How should code instrumentation be done?
- Implement an RV framework prototype. Find a suitable test-like specification language, or design it with inspiration from such languages.
- *(Possible extension)* Apply implemented RV framework on a project at Valtech. Evaluate and analyze. Do some benchmarking to check on how the RV framework impacts performance.

Suggested project(s) at Valtech: The Valtech Intranet (python).

Timeplan/Schedule

I will work on the exjobb 50% and 50% on projects at Valtech, in periods of two weeks exjobb, two weeks work. This fits well into the iteration-planning at Valtech. During the summer I will almost exclusively work on the exjobb, and also use some of my vacation hours for the exjobb.

Suggested approximate time plan:

Start	Weeks	N	Work
May	*1w in May*	**1w**	Writing, and doing the research for, this specification.
May	*2w in May*, v23, v26, v27	**5w**	Doing background & research.
9/7	v28	**1w**	Writing the background part of the report.
16/7	v29, v30, v31, v32	**4w**	Investigating and evaluating "what to do".
13/8	v33	**1w**	Writing about the investigation.
20/8	v34, v35, v36	**3w**	Implementing and evaluating the RV framework.
10/9	v37, v38	**2w**	Testing and analysing the RV framework on "the project".
24/9	v39, v40, v41	**3w**	Writing and finishing the report.

Total: 20 weeks. End date: **12 October 2012** (very optimistic).

I will weeks v24 and v25 off, as well as about 1 week in august (not planned). **The weeks I will be working at Valtech haven't been written into the time table.**

Other required work related to the exjobb, such as doing the opposition of another student's work, will take time from the work above and require flexibility in planning.

Issues

- Who will be the examiner?
- Do I need to start the exjobb work at a specific date and time? Do I need to/Should I take part in an exjobb "support group"?