Comments from Examiner 3:-

Comments on Wu Yongzheng thesis: "Operating System Auditing and Monitoring"

I very much enjoyed reading this doctoral thesis. Especially in terms of the visualization options provided, it was a very exciting thesis.

I appreciated on pages 8 and 9 the list of papers in which the results in this thesis earlier appeared. I would have also appreciated a brief summary of any new results in those sections beyond the published papers, as wall as a list of new results that are being published for the first time in this thesis (whether in those sections or not). While this is not absolutely necessary, it would have been useful to me as a reader (particularly since some of the results here date back to 6 years ago.)

Throughout the text, the present tense is being used. This makes for a slightly strange effect in English when reading sections on testing (for example 6.1.4). The actual tests that you ran were run at a particular point in time in the past, so those results might be better expressed in the past tense. More specifically, there should be a more specific description of the equipment used. For example, again in section 6.1.4, there are many dozen Intel Core Duo processors (see http://www.intel.com/pressroom/kits/quickreffam.htm#core2), and it may be hard to reproduce your results without having more information about the items.

Your bibliography includes URLs that point to non-existent pages (see for example, item 25.) You should go through and fix all of these. I also recommend including a statement in your bibliography such as "all URLs checked as of December 1, 2011" or whenever you actually check them.

Are your tools available online? I would have appreciated some statement about whether you intend to make your tools available, and if relevant, even a brief appendix with instructions on how to download them. Even if you have no intention of making your tools available, at least a supporting web page with details of experimental results would be helpful.

I wish your thesis has a list of open problems (in addition to the summary of results in Chapter 7). There is only an overly brief two paragraph statement about "future work" that is not very compelling. I would have expected at least a couple pages of open problems. This would be a real gift to the field.

It was very strange to read the block remarks at beginning of sections which outline your contributions and other team member contributions in the middle of the thesis (for example, at p. 140 or p. 93 or p. 64 etc.) I respect that you included the information, but by highlighting it this way, it made it look like abstracts for the chapter or section. Instead, I suggest putting this material in a footnote, or in the acknowledgments.

Overall, I loved your thesis. I am confident that the recommendations I suggest in this review will only take a day or two to implement. Advance congratulations on what I am sure will be your newly minted Ph.D.