[WU YONGZHENG (A0002223H)] Comments from Examiner 2 :-

This thesis develop infrastructures, techniques, and applications for operating system auditing and monitoring, which is an important topic for achieving security and reliability of complex modern computer systems.

This thesis first presents host-based monitoring infrastructures for both Linux and Windows systems, namely, Lbox and WinResMon. Compared to existing solutions, the solustion developed in this thesis can monitoring program behaviors transparently and more efficiently. Such infrastructures allow uses to monitor operating system events and resource accesses using a user specification. The solutions are prototyped and evaluated thoroughly.

The thesis also proposes an external monitoring technique to deal with systems compromised by rootkits. Using external sensors, the technique helps a detection system even when the host is compromised with malicious program and thus cannot be relied upon.

Based on the monitoring infrastructures, this thesis develops solutions to visualize system behaviors. The first solution is to graphically represent the component relationships in Windows binaries for better understanding of programs and their behaviors. The second solution compares program behaviors and highlight important behaviors using DotPlot.

To secure a computing environemnt, this thesis also develops novel solutions to eliminate untrusted binary execution. By monitoring the binary loading behavior, such solutions make sure only trusted binaries are executed in a system to prevent execution of malicious code.

The solutions developed in this thesis are novel and comprehensive. The presentation of the thesis is also clear, except for some minor issues. I recommend the award of the Ph.D. degree.

[WU YONGZHENG (A0002223H)] Comments from Examiner 2 :-

The following are comments to the thesis.

1. The external monitoring is a very interesting technique. However, the solution developed in this thesis only use the technique in a simple way. This thesis should give a better discussion of future work along this direction, such as how to integrate the technique with internal monitors to make more accurate decisions. For example, at the end of page 86, discuss how to distinguish local users from remote users in the system: remote users should not run sudo even if there is a local user sitting at the computer.

2. In the introduction, the last paragraph of page 4 is directly duplicated from later sections. It should be rewritten instead. Moreover, at the end of the second paragraph on page 5, the limitation of UAC should be summarized to make the paragraph complete.

3. In section 5.2, page 116, I think the title "visualizing Windows system traces" is not accurate. The section is about the visualization of comparison between Windows traces to highlight important behavior, not the visualization of the trace itself.

On page 116, the second paragraph is not clear. The general functionality of lviz should be described in a little more detail.

4. There are notes right beneath section titles to give information about the candidate's related publications. I suggest to remove the notes and merge citations to related publications in text of the section.

[WU YONGZHENG (A0002223H)] Comments from Examiner 2 :-

5. Some typos and grammar errors:

page 4, last line, citation to DTrace and SystemTap

page 5, 3rd line, The lack of kernel APIs *makes*

page 5, 4th line, in a *hacky* way, which *is*

page 23, last line of 1st paragraph, these tasks *become* more

page 35, first line of 3.1.2.3, the process being *monitored* is