A system protection software base on the virtual restoring technology in Windows operating systems (Shadow Machine)

Jin Yang

(Student Number: 2432777)

September 2016

Dissertation submitted in partial fulfilment for the degree of
Master of Science in Software Engineering

Computing Science and Mathematics
University of Stirling

Abstract

Shadow Machine is a system protection software based on virtual restoring technology. The virtual restoring technology in software is essentially realized through Windows disk filter driver. Firstly Shadow Machine will create a virtual mirror image in the Windows system to realize the isolation and protection of the real system. The operations in the virtual image system and those operations in the real system are identical. But essentially, the operations in the shadow system are virtual, which means that the virus and malware cannot infect the real operation system. All kinds of accidental damages towards the system, for instance, accidental deletion of the files and the useless files left after surfing websites will not be stored. All operations in the virtual mirror image will disappear after the Windows system reboots. If there is a need to modify the system setting, to install new software or to alter some files, the system can be set as normal mode to save all the operations. Then the Windows system can be set to virtual mirror image again to protect the computer and provide the user with a safe environment to work, study and entertain.