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

Jin Yang [jiy00036@students.stir.ac.uk]

MSc in Software Engineering

UNIVERSITY of STIRLING

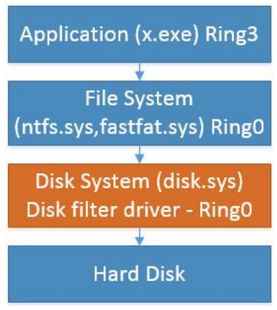
INTRODUCTION

Shadow machine is a piece of Windows system security protection software which is based on virtual restoring technology. When Shadow machine operates it establishes a virtual image model for the current operating system. The user's work in the virtual image model is the same as that in the real operating system while the system automatically rolls back to the previous safe state if the user reboots the computer. This virtual image model is able to completely isolate all kinds of viruses and malwares, together with various kinds of error operations towards Windows operating system.

PROJECT STRUCTURE AND METHODS

Two core technologies of Shadow machine: 1. disk filter driver; 2. flag_table centered disk redirect algorithm.

Windows operating system can be divided into application layer and kernel layer, which respectively corresponds to Ring3 mode and Ring0 mode of the CPU. The specific performance in operating system is that the application layer program(usually .exe file) runs on Ring3 level while driver(usually .sys file) runs on Ring0 level.



Traditionally viruses and malware infect the operating system files, destroying the user data and writing a Trojan or backdoor into the system, the purpose of which is to attack the data of hard disk. To improve protection we should intercept and process these actions and write operations towards the bottom layer disk.

When managing the sectors of the hard disk, Shadow machine abstracts a flag_table, and deposit the flag_table completely into the RAM. Then it puts forward high requirement of the volume of the flag_table.

Hard Disk Sectors	0-31 (32)	32-63 (32)	64-95 (32)	96-127 (32)
Flag Table	0 (1)	1 (1)	2 (1)	3 (1)

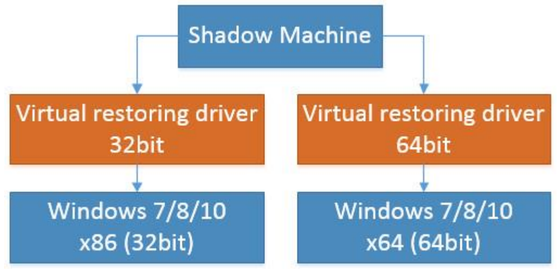
Flag Structure	FlagStatus (1 byte)
	RepIndexFlag (4 byte)
	UseStatus (4 byte)

1 sector is 512 bytes. 1flag is 9 bytes. 1flag can manage 32 sectors, so 9 bytes can manage 16384 bytes. (management efficiency: 1:1820.4444)
For example: a 512G hard disk makes use of 281.318MB of the memory to store flag_table.

OBJECTIVE

The objective of Shadow machine is to protect system security in new way. Shadow machine differs from the traditional anti-virus software, which is based on the anti-virus engine and virus database, in system protection mode. It can be a perfect replacement for the traditional anti-virus software under many application scenarios. It will be a great progress for the anti-virus software industry if Shadow machine is used to protect operating system combined with the traditional anti-virus software.

FUTURE DEVELOPMENT



Shadow machine currently provides 32bit and 64bit virtual restoring driver but 64bit virtual restoring driver does not process digital signature of Microsoft. So it cannot yet run on the 64bit Windows operating system. According to the security mechanism of Microsoft, the digital signature should be applied in the name of the company.
If the application of the digital signature for Shadow machine's 32bit and 64bit virtual restoring driver is granted in the future, Shadow machine will be able to run on the 32bit and 64bit Windows system.