

DESCRIPTION

INFORMATION-PROCESSING DEVICE, INFORMATION-PROCESSING
MONITORING METHOD, ~~PROGRAM,~~ AND RECORDING MEDIUM

Technical Field

[0001] The present invention relates to a technique of monitoring an information processing operation executed by a processor.

Background Art

[0002] Malicious programs have been recently developed to perform unauthorized and harmful operations to a computer, and such malicious programs greatly degrade the security of a computer by replacing a file of the computer or changing the configuration of the system, for example. Such malicious programs behave as follows. They firstly intrude into a memory of the computer from the outside, and piggyback on an access to a resource in the kernel space from a user mode when an application program (AP) is executed. Then they acquire the privilege level (ring 0), and govern the resource control. In this way, unauthorized actions by such programs become executable as the programs intend. Currently various types of software to monitor the execution of malicious programs and control their unauthorized activities are proposed.

[0003] Patent Literature 1 describes a method for monitoring applications to prevent the leakage of resource information. The method is to limit the access by an API, and includes: detecting the starting of an application; suspending a processing request

CLAIMS

1. An information processing device, comprising:

a monitoring unit configured to monitor at least an instruction to pass processing to a kernel of an OS among instructions issued to a processor, and monitor, as a privilege level fault, an access to request for rewriting of a register in which a hook condition is set, the hook condition being for hooking issuance of the instruction and prevent rewriting; and

a load unit configured to load a monitoring software functioning as the monitoring unit at a predetermined region of a main memory, the monitoring software having a privilege level set higher than a privilege level of the kernel of the OS, the load unit including: a first load unit configured to perform loading of the monitoring software after loading of BIOS; and a second load unit included in the monitoring software loaded by the first load unit, the second load unit being configured to perform loading of the kernel of the OS after loading of the monitoring software.

2. The information processing device according to claim 1, wherein

the monitoring unit includes:

a detection unit configured to detect issuance of ~~at least~~
an ~~the~~ instruction to pass processing to the kernel of the OS

~~among instructions issued to the processor;~~

an evaluation unit configured to evaluate validity of the instruction detected; and

a proxy processing unit configured to execute the instruction by proxy in accordance with an evaluation result.

3. The information processing device according to claim 2, wherein the detection unit detects the instruction as an invalid opcode fault.

4. The information processing device according to claim 2 or 3, wherein

the instruction is a Syscall instruction, and

the evaluation unit evaluates validity based on collation with information on an API making up the Syscall instruction.

5. The information processing device according to any one of claims 2 to 4, wherein

the proxy processing unit is configured to, when the evaluation unit determines that the instruction is valid, transfer content identical with the instruction to the kernel, and when the evaluation unit determines that the instruction is invalid, return an instruction to end the instruction to the kernel.

6. The information processing device according to any one of claims 2 to 4, wherein

the proxy processing unit is configured to, when the

evaluation unit determines that the instruction is valid, transfer content identical with the instruction to the kernel, and when the evaluation unit determines that the instruction is invalid, return an instruction to skip the instruction to the kernel.

~~7. The information processing device according to any one of claims 1 to 6, wherein~~

~~the monitoring unit includes a hook condition setting unit to set a hook condition for monitoring, and~~

~~the monitoring unit is configured to detect issuance of at least an instruction to pass processing to the kernel of the OS among instructions issued to the processor based on the hook condition set by the hook condition setting unit.~~

7. The information processing device according to any one of claims 1 to 6, wherein

the monitoring unit includes a hook condition setting unit to set a hook condition for monitoring in the register,
and

the hook condition setting unit includes:

a hook condition monitoring unit configured to monitor an access to request for rewriting ~~rewrite~~ the hook condition;
and

a hook condition correction unit configured to rewrite the hook condition every time issuance of an access to request

for rewriting ~~rewrite~~ the hook condition is detected.

~~9. The information processing device according to any one of claims 1 to 8, wherein~~

~~the load unit includes: a first load unit configured to perform loading of a monitoring software functioning as the monitoring unit; and~~

~~a second load unit included in the monitoring software loaded by the first load unit, the second load unit being configured to perform loading of the kernel of the OS.~~

~~108.~~ The information processing device according to any one of claims 91 to 7, wherein the first load unit is configured to load the monitoring software functioning as the monitoring unit at privilege level 0, and the second load unit is configured to load the kernel of the OS at any one of privilege levels 1 and 2.

~~11. A method for monitoring information processing, comprising:~~

~~monitoring at least an instruction to pass processing to a kernel of an OS among instructions issued to a processor; and~~

~~loading a monitoring software functioning as the monitoring step at a predetermined region of a main memory, the monitoring software having a privilege level set higher than a privilege level of the kernel of the OS.~~

~~12. A program that makes a processor function as:~~

~~a monitoring unit configured to monitor at least an instruction to pass processing to a kernel of an OS among instructions issued to the processor; and~~

~~a load unit configured to load a monitoring software functioning as the monitoring unit at a predetermined region of a main memory, the monitoring software having a privilege level set higher than a privilege level of the kernel of the OS.—~~

~~[13] A computer readable recording medium that records a program to make a processor function as:~~

~~a monitoring unit configured to monitor at least an instruction to pass processing to a kernel of an OS among instructions issued to the processor; and~~

~~a load unit configured to load a monitoring software functioning as the monitoring unit at a predetermined region of a main memory, the monitoring software having a privilege level set higher than a privilege level of the kernel of the OS.~~

9. The information processing device according to claim 2, wherein the proxy processing unit executes the instruction by proxy irrespective of validity of an evaluation result.

10. The information processing device according to claim 7, wherein the hook condition correction unit is configured to rewrite a hook condition in the register when rewriting of the

hook condition in the register is detected.

11. A method for monitoring information processing, comprising:

instruction monitoring at least an instruction to pass processing to a kernel of an OS among instructions issued to a processor,

hook condition monitoring, as a privilege level fault, an access to request for rewriting of a register in which a hook condition is set, the hook condition being for hooking issuance of the instruction and preventing rewriting; and

loading a monitoring software functioning as the instruction monitoring and the hook condition monitoring at a predetermined region of a main memory, the monitoring software having a privilege level set higher than a privilege level of the kernel of the OS, the loading including: first loading of loading of the monitoring software after loading of BIOS; and second loading included in the monitoring software loaded at the first loading, the second loading being to perform loading of the kernel of the OS after loading of the monitoring software.

12. A computer readable recording medium that records a program to make a processor function as:

a monitoring unit configured to monitor at least an instruction to pass processing to a kernel of an OS among instructions issued to a processor, and monitor, as a privilege

level fault, an access to request for rewriting of a register in which a hook condition is configured, the hook condition being for hooking issuance of the instruction and prevent rewriting; and

a load unit configured to load a monitoring software functioning as the monitoring unit at a predetermined region of a main memory, the monitoring software having a privilege level set higher than a privilege level of the kernel of the OS, the load unit including: a first load unit configured to perform loading of the monitoring software after loading of BIOS; and a second load unit included in the monitoring software loaded by the first load unit, the second load unit being configured to perform loading of the kernel of the OS after loading of the monitoring software.