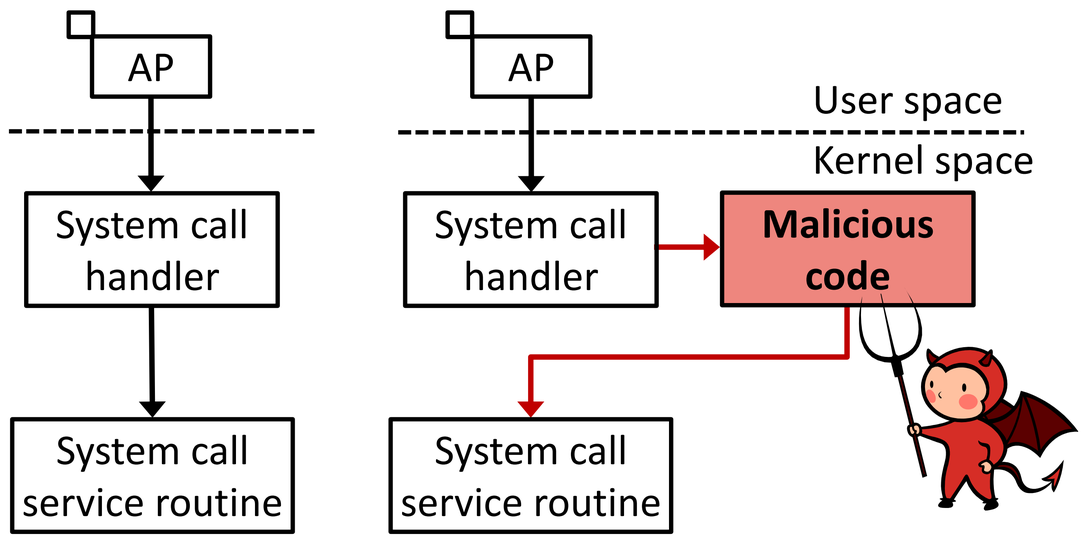
Proposal of Kernel Rootkit Detection by Monitoring Branches Using Hardware Features

Yohei Akao and Toshihiro Yamauchi
(Graduate School of Natural Science and Technology, Okayama University)
Email: akao@swlab.cs.okayama-u.ac.jp

1. Introduction

- When a computer system is infected with a kernel rootkit, attack detection is difficult
- Traditional kernel rootkit detection methods do not resolve all of the following problems simultaneously:
  (1) cannot detect kernel rootkits immediately
  (2) cannot keep the scalability of the OS kernel
  (3) cannot extend to different OS and OS versions
  (4) cannot detect kernel rootkits that use instructions that do not push data into the kernel stack (e.g., jmp)
- Many kernel rootkits make branches that differ from the usual branches in kernel space



(a) System call not infected with the kernel rootkits (b) System call infected with the kernel rootkits

Figure 1. Changes in the control-flow when system call control-flow is modified

2. Kernel Rootkit Detection by Monitoring Branches Using Hardware Features

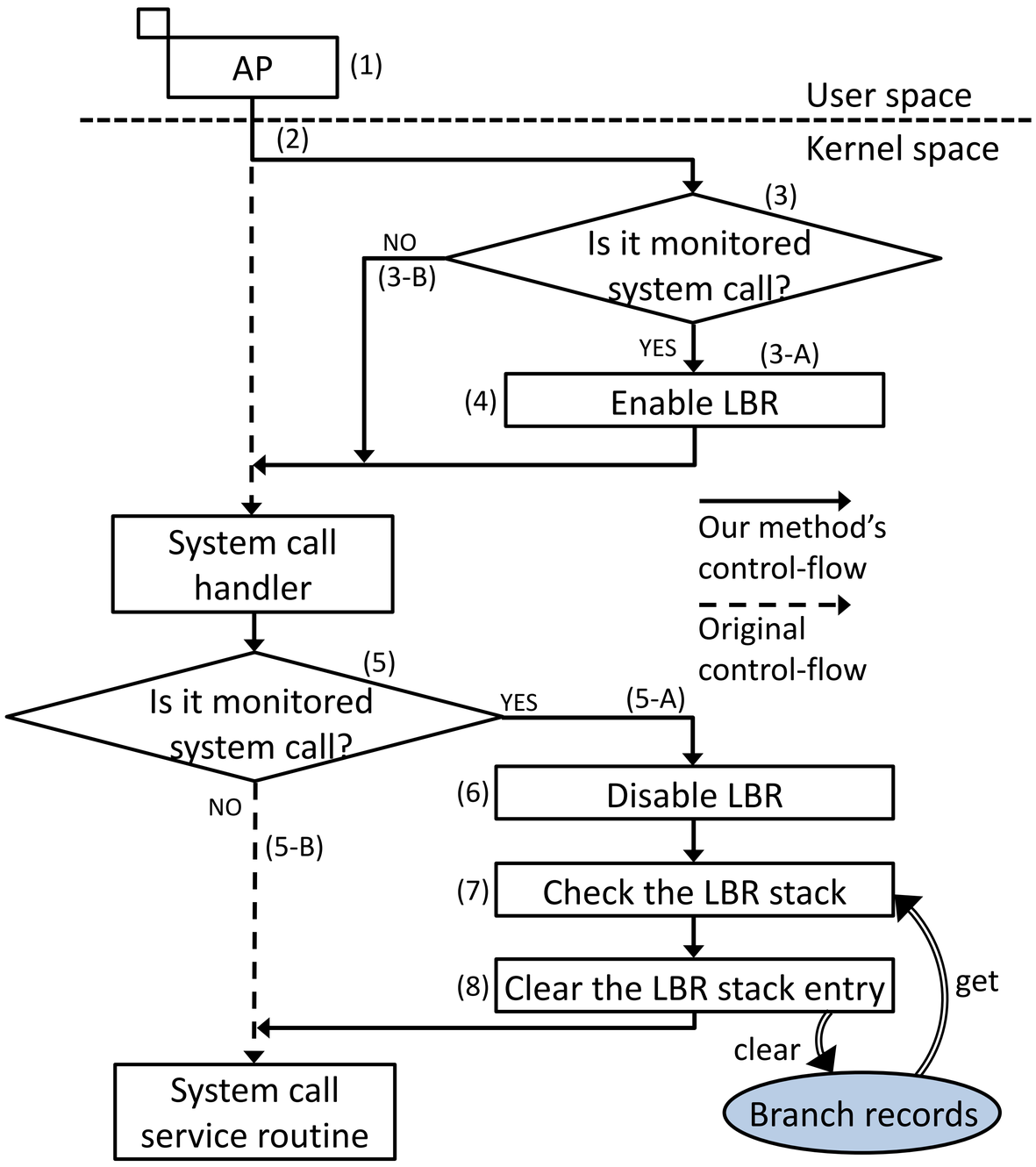


Figure 2. Processing flow of our method

■ Concept

Previous researches indicate that many kernel rootkits employ control-flow modification, making branches different from usual. Then, our method detects kernel rootkits by monitoring branch records in kernel space and by detecting control-flow modification. Our method uses Last Branch Record (LBR), a recent feature of Intel processors for monitoring the branch records.

■ Last Branch Record

When LBR is enabled, the CPU records the address of a branch instruction and its target instruction. LBR can store 16 entries. When more than 16 entries are recorded, the oldest stack data is overwritten. Monitoring branch records using LBR has the following advantages:

(1) It can record all branch records in the kernel.
Therefore, it can monitor branch records recorded by instruction that do not push data into the kernel stack.

(2) It is transparent to the OS structure.

(3) It generates minimal overhead.

■ How to detect kernel rootkit

- When a computer system is infected with a kernel rootkit, a quantity of branch records recorded by LBR increases.
- Our method monitors the branch records between the invoking a system call and the transition to each system call service routine.

Our method detects kernel rootkits that modify the control-flow of the system call by monitoring an increase in a quantity of branch records.

3. Conclusion

- We proposed the efficient way to detect kernel rootkits using hardware features.
- Our method detects kernel rootkits by monitoring branch records in kernel space using LBR.
- Our method resolves all problems (1) – (4) simultaneously.