Abstract

The recent interest in runtime attestation requires modeling of a program’s runtime behavior to formulate its integrity properties. In this work, we study the possibility of employing static source code analysis to derive integrity models of a commodity operating systems kernel. We develop a precise and static analysis-based global invariant detection tool that overcomes several technical challenges: field-sensitivity, array-sensitivity, pointer analysis, and handling of assembly code. We apply our tool to Linux kernel 2.4.32 and identify 141,279 global invariants that are critical to its runtime integrity. Furthermore, comparison with the result of a dynamic invariant detector reveals 17,182 variables that can cause false alarms for the dynamic detector. Our experience suggests that static analysis is a viable option for automated integrity property derivation, and it can have very low false positive rate (1 out of 141,280 in our Linux kernel case study) and very low false negative rate (18 out of 141,297).

Problem Statement

- Trust Issues in Computer Systems
  - Constant attacks exploiting vulnerabilities (e.g. buffer overflow, SQL injection)
  - Privilege escalation due to configuration errors
  - Malware (e.g., rootkits) increasingly stealthy

- Current Solution: Integrity Checks through Remote Attestation

- Challenge of Runtime Attestation: Precision of Integrity Models
  - Integrity guarantee is only as strong as the completeness of the integrity model. E.g., if integrity properties only cover system call table, a new rootkit can manipulate other function pointers (such as those found in device driver jump tables) to achieve its goal and remain undetected
  - If the integrity model is too restrictive, the detector may report too many false alarms

- Our Contributions
  - A precise program analysis tool that can automatically derive global invariants from source code, using static analysis
  - A thorough study of global invariants detection for the Linux kernel
  - An invariant monitor based on the result of the static analysis with low false positive and false negative rates