Fast Object Naming for Kernel Data Anomaly Detection
Hayoon Yi*, Yeongpil Cho*, Donghyun Kwon*, Yunheung Paek*
*Seoul National University

- Memory Introspection
- Backtrace Naming
  Backtrace: a backward list of active function calls that starts with the last function call
  Naming: Giving an identity to a data object to distinguish it from other objects with different names.
- Naming Granularity
  How would different naming schemes affect the granularity of which data objects would be distinguishable
  - Path-name
  - Type-name
  - Backtrace-name
- Key Observations
  1. Kernel objects are allocated through only a couple of fundamental object allocators.
  2. The kernel context when a kernel object is created reflects the object’s characteristic during runtime.
- Preliminary Experiments
  - The number of allocations: 186,132
  - The number of deallocations: 156,367
  - The number of live objects: 29,765
  - Avr. CPU cycles per trap: 321
  - Avr. CPU cycles per backtrace-naming: 140
  - Total spent CPU cycles of traps: 116,440,503
  - Total spent time (ms) of traps at 1.7GHz: 68.49

- Motivation
  - Deployed security systems usually rely on integrity specifications, which are typically set by a security administrator
  - Non-control data attacks in kernel
  - Need for kernel data integrity
  - Unfortunately, it is nontrivial to manually set specifications for all kernel data
  - Automated specification generation with machine learning
  - Prior work was done in this area
    - Has an issue that a large portion of generated specifications not being applicable after a system reboot
    - Needs to re-generate specifications after each reboot, which takes 20~50 minutes even on an up-to-date machine

- Prototype Overview

- Backtrace extraction at an allocation event

- Acknowledgements
  This work was partly supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (No. 2014R1A2A1A1051792), Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No. 80190-16-2010, Development on the SW/HW modules of Processor Monitor for System Intrusion Detection)and Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP) (No. R-20160222-002755, Cloud based Security Intelligence Technology Development for the Customized Security Service Provisioning)