Fine-grained OS Behavior Characterization

Lorenzo Cavallaro, Cristiano Giuffrida, and Andrew S. Tanenbaum
{sullivan,giuffrida,ast}@cs.vu.nl
Vrije Universiteit, Amsterdam, The Netherlands

Research Proposal

Problem

- Systems' behavior characterization has important reliability and security applications
  (e.g., malware detection)
- Unfortunately, it is usually **hard** to characterize the behavior of complex systems
  (e.g., monolithic operating systems)

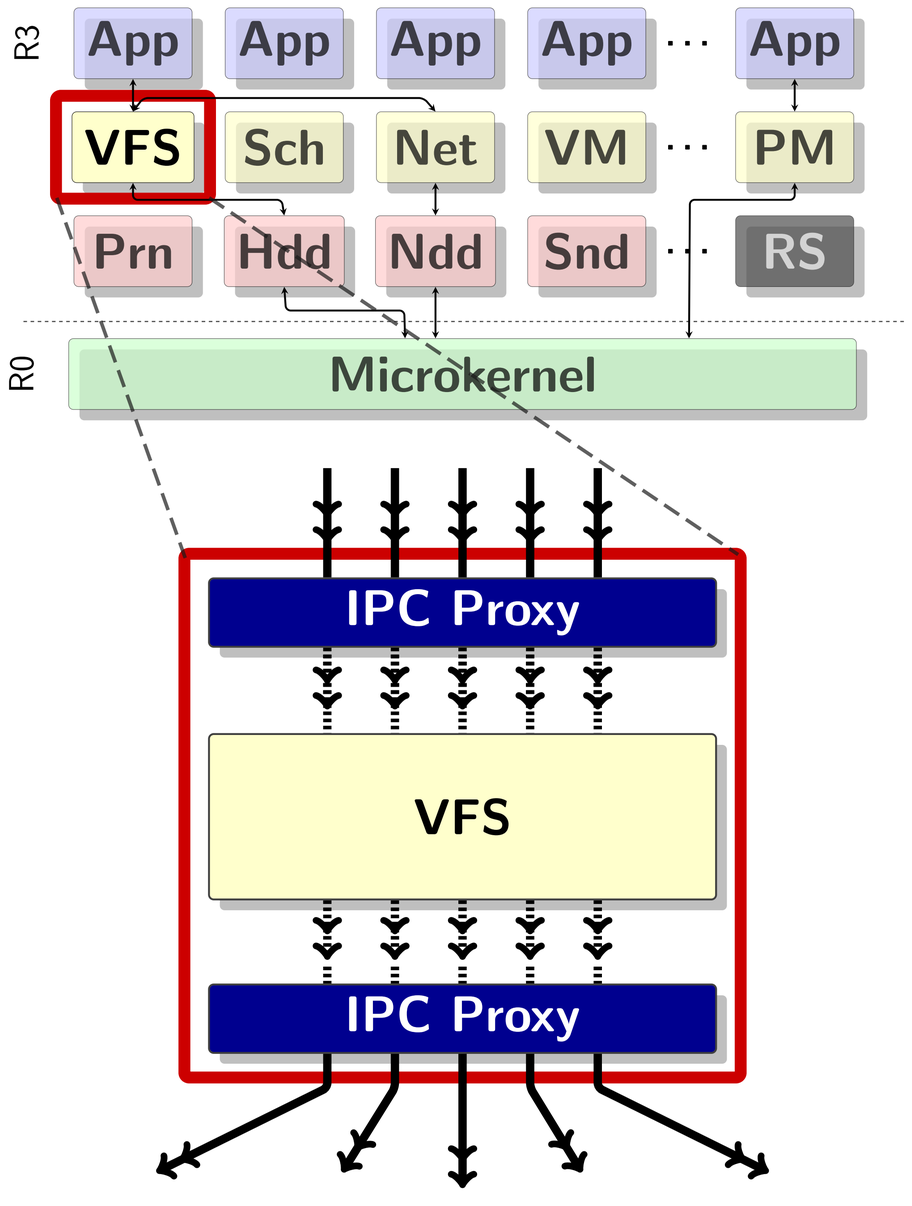
Goal

- Design a multiserver microkernel-based OS
- OS components communicate via message passing (IPC) and run as userspace processes
  - Carry out **specific** tasks by design
  - Behavior may be easy to characterize in a short time
    (i.e., contrary to arbitrary userspace processes)

Approach

- IPC-based monitoring infrastructure
  - Create fine-grained behavioral profiles $\mathcal{P}$ of the OS
    (classic profiling or learning phase)
  - Exploited to match $\mathcal{P}$ against the observed run-time behavior of the OS components
    (classic detection phase)

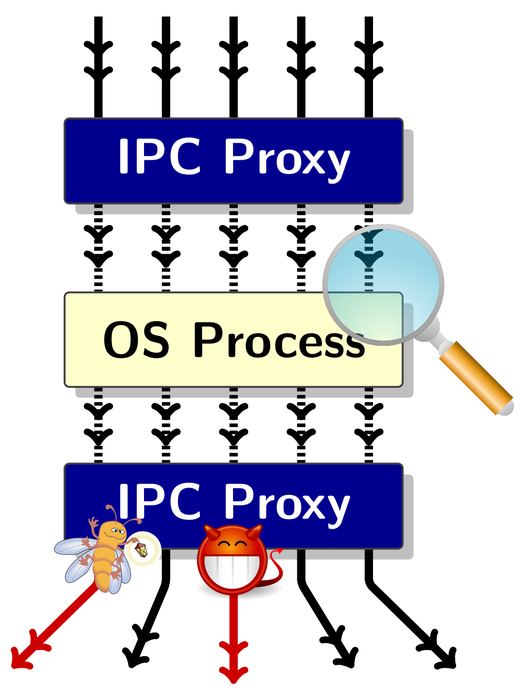
OS Architecture



Multiserver microkernel-based OS and IPC monitoring infrastructure

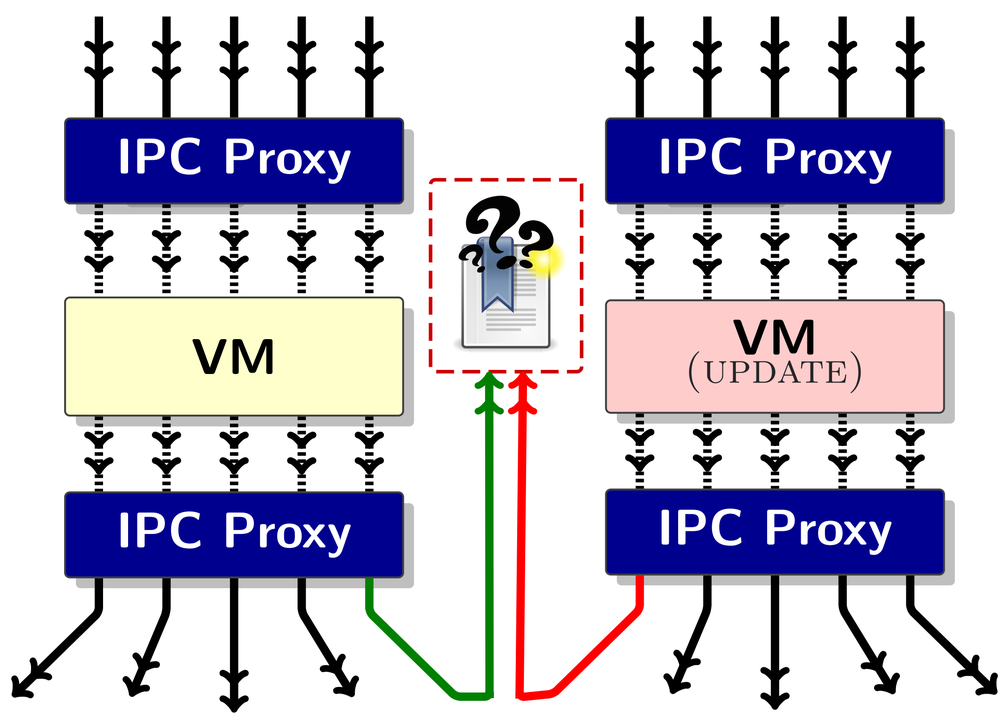
Possible Applications

Anomalous Behavior Detection



Detect malicious and buggy behavior by comparing it against the learnt IPC profile

Online Patch Validation



Compare IPC differences against a given OS component update specification

Understanding the behavior of the entire OS opens up interesting research directions

Supported by European Research Council under grant ERC Advanced Grant 2008 - R3S3