EXTENDED BERKELEY PACKET FILTER FOR INTRUSION DETECTION IMPLEMENTATIONS

William Findlay

School of Computer Science, Carleton University

System introspection is becoming an increasingly attractive option for maintaining operating system stability and security. This is primarily due to the many recent advances in system introspection technology; in particular, the 2013 introduction of *Extended Berkeley Packet Filter* (*eBPF*) into the Linux Kernel along with the recent development of more usable interfaces such as the *BPF Compiler Collection* (*bcc*) has resulted in a highly compelling, performant, and (perhaps most importantly) safe subsystem for both kernel and userland instrumentation.

The scope, safety, and performance of eBPF system introspection has potentially powerful applications in the domain of computer security. In order to demonstrate this, we present *ebpH*, an eBPF implementation of Somayaji's *Process Homeostasis* (*pH*). ebpH is an intrusion detection system (IDS) that uses eBPF programs to instrument system calls and establish normal behavior for processes, building a profile for each executable on the system; subsequently, ebpH can warn the user when it detects process behavior that violates the established profiles.

This poster will discuss the design and implementation of ebpH along with the technical challenges which occurred along the way. We will present experimental data and performance benchmarks that demonstrate ebpH's ability to monitor process behavior with minimal overhead. Finally, we conclude with a discussion on the merits of eBPF IDS implementations and potential avenues for future work therein.