Extended Berkeley Packet Filter for Intrusion Detection

Honours Thesis Proposal

William Findlay

October 4, 2019

Abstract

Since its introduction to the Linux Kernel in 2013 [1], *Extended Berkeley Packet Filter* (eBPF) has provided a powerful toolkit for GNU/Linux developers to perform powerful system introspection and monitoring. This is thanks largely in part to its guaranteed safety, as well as its ability to inspect any kernel data structure in real time [1], [2]. Additionally, its ever-expanding set of features [2] as well as projects like *bcc* [3] are set to ensure that eBPF is more powerful and accessible than ever before in the years to come.

While eBPF is certainly ideal for performance monitoring use cases, there is no reason to stop there; powerful and safe system introspection techniques can offer promising boons to many fields, including that of computer security. The aim of this thesis is to provide an argument for eBPF's effectiveness in the domain of computer security. In particular, I hope to show that eBPF tracing programs can be leveraged effectively and efficiently for intrusion detection system implementations.

1 Introduction

1.1 Background

References

[1] A. Starovoitov, "Tracing filters with bpf," The Linux Foundation, RFC 0/5, Dec. 2013. [Online]. Available: https://lkml.org/lkml/2013/12/2/1066.

[2] S. Goldstein, "The next linux superpower: Ebpf primer," USENIX SRECon16 Europe, Jul. 2016. [Online]. Available: https://www.usenix.org/conference/srecon16europe/program/presentation/goldshtein-ebpf-primer.

[3] *Iovisor/bcc*, Oct. 2019. [Online]. Available: https://github.com/iovisor/bcc.