Extended Berkeley Packet Filter for Intrusion Detection Implementations

COMP4906 Honours Thesis Proposal

by

William Findlay

November 3, 2019

Under the supervision of Dr. Anil Somayaji
Carleton University

Abstract

Acknowledgments

Contents

1 Introduction **1**
1.1 Motivation . . . 1
1.2 System Introspection and Observability . . . 1

2 Background **1**
2.1 Extended Berkeley Packet Filter . . . 1
2.1.1 Linux Superpowers . . . 1
2.1.2 The Verifier . . . 1
2.1.3 eBPF Programs . . . 1
2.1.4 XDP Programs . . . 1
2.2 Intrusion Detection . . . 1
2.3 Process Homeostasis . . . 1

3 Implementing ebpH **1**

4 Methodology **1**

References **2**

Appendix Testificate **3**

List of Figures

List of Tables

List of Listings

1 Introduction

1.1 Motivation

1.2 System Introspection and Observability

2 Background

2.1 Extended Berkeley Packet Filter

2.1.1 Linux Superpowers

2.1.2 The Verifier

2.1.3 eBPF Programs

2.1.4 XDP Programs

2.2 Intrusion Detection

2.3 Process Homeostasis

3 Implementing ebpH

4 Methodology

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.

Appendix A Testificate