Last Updated: February 14, 2020

William Findlay

github.com/willfindlay ● williamfindlay.com
(613) 296-1240 ● william@williamfindlay.com

Education

Bachelor of Computer Science *Carleton University*
September 2015 - April 2020 *Ottawa, ON*
Computer and Network Security Stream
Accelerated Masters Program
CGPA: 11.0 (A)

Work Experience

Undergraduate Researcher (Linux OS Security) *Carleton University*
April 2019 - Present *Ottawa, ON*

- Researching the viability of eBPF-based implementations for intrusion detection systems on the GNU/Linux operating system.
- Designed and implemented ebpH, an intrusion detection system based entirely on eBPF system introspection.
- This research is the subject of my 2019/2020 honors thesis. You can read my thesis proposal at https://williamfindlay.com/written/thesis-proposal.pdf.

Teaching Assistant (COMP3000 Operating Systems) *Carleton University*
September 2018 - Present *Ottawa, ON*

- Nominee for the Outstanding Teaching Assistant Award
- Assisted the professor in development of course material.
- Ran tutorial sessions for groups of 50 students.
- Took a leadership role to ensure tutorials proceeded smoothly.
- Held weekly office hours and workshops for students.
- Graded assignments and tests and gave appropriate feedback.

Service Department Supervisor *Metro Ontario, Inc.*
April 2014 - January 2018 *Ottawa, ON*

- Managed day-to-day operations in the front end service department.
- In charge of store payroll and accounting on a part-time basis.
- Exhibited superior customer service skills as required.

Projects (See more on GitHub)

ebpH (eBPF Intrusion Detection System)

- An intrusion detection system for Linux written entirely in eBPF and Python3.
- Establishes per-executable system call profiles in order to establish normal behavior and detect anomalies.
- Full source code available at https://github.com/willfindlay/ebph.

Snoopy (eBPF Debugger)

- System call tracing debugger written in eBPF and Python3.
- Competitor to strace, with much higher performance due to lack of reliance on the ptrace system call.
- Full source code available at https://github.com/willfindlay/snoopy.

bpf-keylogger (eBPF Keylogger Program)

- Fully functional keylogger for GNU/Linux written in eBPF and Python3.
- Full source code available at https://github.com/willfindlay/bpf-keylogger.

Languages

Programming
10,000 or more lines
C, C++, Python

5,000 - 10,000 lines
Java, Javascript

1,000 - 5,000 lines
Haskell, Prolog, Vimscript, R, Common Lisp

Markup
Markdown, Rmarkdown, LaTeX, HTML, CSS

Human
English, French

Workflow

Operating System
GNU/Linux (Arch Linux)

Window Manager
i3wm

Shell
Zsh

Text Editor
Vim

Version Control
Git, GitHub

Technologies

- eBPF, XDP, bcc
- gdb
- flask
- numpy, scipy, pandas
- Qt

Technical Skills

- Linux kernel development
- Low level systems programming
- Python scripting
- Technical writing and documentation

General Skills

- Team leader
- Dedicated
- Goal-oriented