William **Findlay**

SECURITY RESEARCHER · SYSTEMS PROGRAMMER · KERNEL HACKER

(613) 296-1240 | william@williamfindlay.com | www.williamfindlay.com | willfindlay | in willfindlay

Education

Carleton University
DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

Ottawa, Canada
Sept. 2021 – Present

- Current CGPA: Pending
- Thesis: Pending

Carleton University
MASTER OF COMPUTER SCIENCE

Ottawa, Canada
Sept. 2020 – Aug. 2021

- CGPA: 12.00 (A+)
- Accelerated Master's Program
- Research focused on operating system and container security
- Nominated for a Senate medal for academic achievement (decision pending)
- Thesis: A Practical, Flexible, and Lightweight Confinement Framework in eBPF

Carleton University
B.Sc. COMPUTER SCIENCE, HONOURS

Ottawa, Canada
Sept. 2015 – Apr. 2020

- CGPA: 11.05 (A)
- Accelerated Master's Program
- Graduated with High Distinction, Dean's Honour List
- Thesis: Host-Based Anomaly Detection with Extended BPF

Skills

Linux Kernel	Kernel Hacking, Kernel Module Development, eBPF, XDP, bcc, libbpf
Systems Programming	C, C++, Rust
Data Science	Pandas, Numpy, Scipy, R
Research	Applied Security, Operating System Security, Sandboxing, Intrusion Detection

Languages

Programming	C, Rust, Python
Human	English, French

Academic Experience

Carleton University
RESEARCH ASSISTANT

Ottawa, Canada
Apr. 2019 – Present

- Member of the CCSL/CISL research group.
- Researching Extended BPF for runtime security implementations under the Linux kernel.
- Co-supervised by Dr. Anil Somayaji and Dr. David Barrera.
- Designed and developed ebpH, an anomaly detection system for Linux, using eBPF.
  - ▸ This work was the subject of my undergraduate Honours Thesis.
- Designed and developed bpfbox, a process confinement tool for Linux, using eBPF.
  - ▸ This work was published at ACM CCSW'2020.

Carleton University
TEACHING ASSISTANT, COMP4000/5012 DISTRIBUTED OPERATING SYSTEMS

Ottawa, Canada
Sept. 2021 – Present

- Assisted the professor with planning and developing course material for a 50 student mixed graduate and undergraduate seminar course
- Created bi-weekly quizzes based on the content of research papers
- Designed two implementation experiences for students, focused around Kubernetes deployments in the cloud
- Graded assignments, term papers, and exams

Carleton University   *Ottawa, Canada*
Head Teaching Assistant, COMP3000 Operating Systems   *Sept. 2018 – Sept. 2021*

- Nominee for the Outstanding Teaching Assistant Award in the 2018/2019, 2019/2020, and 2020/2021 academic years.
- 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.
- Developed a Discord bot to help manage the class Discord server, used during the COVID-19 pandemic.
- Developed new tutorials which are now used each semester:
  - Concurrency tutorial
  - Kernel memory management tutorial
  - eBPF tutorial
  - Rootkit tutorial

Other Experience

Metro Ontario, Inc.   *Ottawa, Canada*
Customer Service Supervisor   *Apr. 2014 – Jan. 2018*

- 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.

Awards and Nominations

Accolades

2021	**Nominee**, Senate Medal for Academic Achievement, Carleton University	*Ottawa, Canada*
2021	**Nominee**, Outstanding Teaching Assistant Award, Carleton University	*Ottawa, Canada*
2020	**Nominee**, Outstanding Teaching Assistant Award, Carleton University	*Ottawa, Canada*
2019	**Nominee**, Outstanding Teaching Assistant Award, Carleton University	*Ottawa, Canada*
2020	**Recipient**, Dean's Honour List, Carleton University	*Ottawa, Canada*
2019	**Recipient**, Dean's Honour List, Carleton University	*Ottawa, Canada*

Scholarships

2020	**Recipient**, Domestic Entrance Masters ($2,000 CAD), Carleton University	*Ottawa, Canada*
2020–2021	**Recipient**, Departmental Scholarships ($6,000 CAD / year), Carleton University	*Ottawa, Canada*
2020–2021	**Recipient**, Research Assistants ($6,000 CAD / year), Carleton University	*Ottawa, Canada*
2020–2021	**Recipient**, Teaching Assistants ($11,000 CAD / year), Carleton University	*Ottawa, Canada*
2015–2019	**Recipient**, Entrance Scholarship ($2,000 CAD / year), Carleton University	*Ottawa, Canada*

Presentations and Invited Talks

Invited Talk, IBM Research – Security and Privacy   *Virtual Event, USA*

- Invited guest speaker for the IBM Security and Privacy research group.
- Discussed my work on bpfbox, a process confinement mechanism for Linux using eBPF.
- Presented an overview of process confinement, eBPF, and its applications to security.

Conference Presentation, ACM CCSW'2020 *Virtual Event, USA*
BPFBOX: SIMPLE PRECISE PROCESS CONFINEMENT WITH EBPF *Nov. 2020*
- Presented my work and accompanying paper on bpfbox, a process confinement mechanism for Linux using eBPF.

Seminar Presentation, CCSL/CISL Seminar *Ottawa, Canada*
BPFBOX: SIMPLE PRECISE PROCESS CONFINEMENT WITH EBPF *Oct. 2020*
- Speaker at a seminar for the CCSL/CISL research group.
- Discussed my work on bpfbox, a process confinement mechanism for Linux using eBPF.
- Presented an overview of process confinement, eBPF, and its applications to security.

Lightning Talk, First Annual eBPF Summit *Virtual Event, USA*
BPFBOX: SIMPLE PRECISE PROCESS CONFINEMENT WITH EBPF AND KRSI *Oct. 2020*
- Invited to give a lightning talk for the inaugural eBPF summit, hosted by Cilium.
- Gave a brief talk about my work on bpfbox, a process confinement mechanism for Linux using eBPF.

Seminar Presentation, CCSL/CISL Seminar *Ottawa, Canada*
EXTENDED BPF PROCESS HOMEOSTASIS *Apr. 2020*
- Speaker at a seminar for the CCSL/CISL research group.
- Discussed my work on ebpH, an anomaly detection system for Linux using eBPF.
- Presented an overview of anomaly detection, eBPF, and its applications to security.

Publications

CONFERENCE PROCEEDINGS

[1] William Findlay, Anil Somayaji, and David Barrera. "bpfbox: Simple Precise Process Confinement with eBPF". In: *Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop*. CCSW'20. Virtual Event, USA: Association for Computing Machinery, 2020, pp. 91–103. DOI: 10.1145/3411495.3421358.

TECHNICAL REPORTS, ARCHIVES, AND THESES

[1] William Findlay. "Host-Based Anomaly Detection with Extended BPF". Honours Thesis. Carleton University, 2020. URL: https://www.cisl.carleton.ca/~will/written/coursework/undergrad-ebpH-thesis.pdf.

Open-Source Software

CREATOR/MAINTAINER

BPFContain
EXPERIMENTAL CONTAINER SECURITY MECHANISM USING eBPF
- Designed and implemented a container security framework using eBPF programs and LSM hooks.
- Tech stack for this project includes Rust, libbpf-rs, and eBPF.
- BPFContain is the subject of ongoing research and development, and will be the topic of my 2021 Master's Thesis.
- Full source code available: https://github.com/willfindlay/bpfcontain-rs

bpfbox
eBPF-BASED PROCESS CONFINEMENT MECHANISM
- Designed and implemented the first eBPF-based policy enforcement engine and a high-level policy language for process confinement.
- This work was published at ACM CCSW'2020.
- Full source code available: https://github.com/willfindlay/bpfbox

ebpH
eBPF-BASED INTRUSION DETECTION SYSTEM
- Designed and implemented an intrusion detection system for Linux based on eBPF.
- Establishes per-executable system call profiles in order to establish normal behaviour and detect anomalies.
- Full source code is available: https://github.com/willfindlay/ebpH

CONTRIBUTOR

bcc
eBPF PROGRAMMING FRAMEWORK FOR PYTHON
- Regular contributor to a large open-source project.
- Implemented the following major features:
  - Support for the ringbuf eBPF map
  - Enhanced support for LSM probes
  - Python support for stack and queue eBPF maps
- Full source code is available: https://github.com/iovisor/bcc.

libbpf-rs
RUST IMPLEMENTATION OF libbpf
- Implemented several major features to an open-source Rust project:
  - Support for the ringbuf eBPF map
  - Enhanced support for LSM probes
  - Bugfixes and general API improvements
- Full source code is available: https://github.com/libbpf/libbpf-rs.