William **Findlay**

SECURITY RESEARCHER · SYSTEMS PROGRAMMER · KERNEL HACKER

☎ (613) 296-1240 | ✉ william@williamfindlay.com | ⌂ www.williamfindlay.com | willfindlay | willfindlay

Education

Carleton University
Ottawa, Canada

MASTER OF COMPUTER SCIENCE
Sept. 2020 – Present

- Current CGPA: 12.00 (A+) (Some course work completed during undergrad)
- Accelerated Master's Program

Carleton University
Ottawa, Canada

B.SC. COMPUTER SCIENCE, HONOURS
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, Python, Rust, C++, Java, Javascript, R
Markup	LaTeX, HTML, CSS
Human	English, French

Academic Experience

Carleton University
Ottawa, Canada

RESEARCH ASSISTANT
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
Ottawa, Canada

TEACHING ASSISTANT, COMP3000 OPERATING SYSTEMS
Sept. 2018 – Present

- Nominee for the Outstanding Teaching Assistant Award in both the 2018/2019 and 2019/2020 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

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

BPFBOX: SIMPLE PRECISE PROCESS CONFINEMENT WITH EBPF

Dec. 2020

- 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

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.

pybpf

Experimental libbpf Bindings for Python

- Designed and implemented an experimental eBPF framework for Python with support for CO-RE and libbpf bindings.
- Full source code is available: https://github.com/willfindlay/pybpf.

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.