OLIVIA LUCCA FRASER

CONTACT INFORMATION

ADDRESS	43 Union Street, Sackville, New Brunswick, E4L 4M6
EMAIL	lucca.fraser@gmail.com
GITHUB	https://github.com/oblivia-simplex
PHONE	1-902-222-7378

SUMMARY

Sept. '21 – PRESENT STAFF RESEARCH ENGINEER ON TENABLE'S ZERO DAY RESEARCH TEAM. I reverse engineer various software and hardware products to discover previously unknown vulnerabilities, and then disclose these issues to the vendors and the public following Tenable's responsible disclosure protocol. Notable achievements include the discovery of a series of vulnerabilities that can be used to achieve root access on every Phicomm router on the market, the development of reverse engineering tools that leverage state of the art Large Language Models (LLMs) to assist in binary analysis, and the discovery and repair of numerous command injection vulnerabilities in Tenable's own plugin feed, protecting our entire customer base from attack before these vulnerabilities became known to malicious actors. I have presented my research at the Atlantic Security Conference in 2022 and at Recon Montreal in 2023, and have published several technical posts on the Tenable Techblog, to bring my research to a wider audience.

Jun. '19 – Sept. '21 INDEPENDENT CONSULTING SOFTWARE ENGINEER AND COMPUTER SCIENTIST, self-employed under 3328018 Nova Scotia Limited.

From June, 2019, to June 2020, I helped Kraken (a major cryptocurrency exchange) port its back-end codebase from PHP to Rust, dramatically improving both its efficiency and security. (Details can be provided upon request.)

From June 2020 to the present, I've been leading research teams under the aegis of the startup, SPECIAL CIRCUMSTANCES, on two high-profile DARPA contracts. The first, ARTIFICIAL INTELLIGENCE MITIGATIONS OF EMERGENT EXECUTION (AIMEE), concerns the exploration of the space of software exploits or "weird machines" by means of genetic programming (GP) and reinforcement learning (RL). The second, RECOVERY OF SYMBOLIC MATHEMATICS FROM CODE (ReMath), concerns the use of constraint-guided symbolic regression to assist in reverse engineering abstract specifications from programmable logic controllers (PLCs), facilitating security audits of industrial control systems (ICS).

Nov. '16 – Jun. '19 VULNERABILITY RESEARCHER AND SOFTWARE ENGINEER at TENABLE NETWORK SECURITY, in the Language Tools and Libraries department. While there, I contributed a number of analytical tools to the company, developed a utility library for collection data types and higher order functions in NASL, and helped to rebuild our SSH library from scratch. Since 2017, my primary responsibility has been to design and implement a suite of testing and static analysis tools for Nessus plugins, including an integration testing framework 'flatline', and a syntactic linter called 'pedant2', both written in Python, and

a semantic bytecode analysis engine known as 'ADAPT', written in OCaml. I also pick up reverse engineering projects from our Zero Day Research department on a regular basis, where I have discovered vulnerabilities in a well-known antivirus that permit an attacker to escape a sandboxed VM (CVE forthcoming).

Jun. '16 – Nov. '16 Quality assurance engineer and researcher at Tenable Network Security. I was responsible for thoroughly testing and debugging Nessus plugins before they were pushed to the feed. During my time in QA, I also developed an extensive, distributed performance profiling system that allowed our department to pinpoint critical bottlenecks, and improve the running time of numerous plugins by orders of magnitude.

Sep. '15 – present Graduate student and researcher at the NIMS Laboratory at Dalhousie University.[1] My research focuses on evolutionary computation in offensive security. I am currently developing a system called ROPER (*Return Oriented Program Evolution in ROPER*), which implements a form of genetic programming to compile (or, rather, evolve) ROP-chains[2] that exhibit complex and adaptive behaviour.

Programming languages and styles

Functional	OCaml, Lisp (Common Lisp, Clojure, Scheme, etc.)
Procedural	C, Rust
Assembly	x86, AMD64, ARM, MIPS
Object-Oriented	Python, Java
Scripting	Bash, NASL, BASIC
Declarative	Prolog
Markup	HTML, CSS, & LaTeX

Education

2015 – 2018
Master of Computer Science
Dalhousie University (NIMS Laboratory), Halifax, NS
Thesis Project: Urschleim in Silicon: Return Oriented Program Evolution with ROPER

2011 – 2013
Researcher at the Jan van Eyck Academie
Maastricht, Netherlands
Organizer of *Versus Laboratory* research project

2008 – 2014
PhD in Philosophy (partial, abd)
University of Guelph, Guelph, Ontario
Dissertation: *Formalization and Dialectics*
Supervisors: Profs. Jay Lampert and Emmanuel Barot

2004 – 2007
MA in Philosophy, graduated with distinction
Brock University, St. Catharines, Ontario
Thesis: *This Infinite Unanimous Dissonance: A Study in Mathematical Existentialism, through the Work of Jean-Paul Sartre and Alain Badiou*
Supervisor: Prof. Rohit Dalvi
External examiner: Dr. Ray Brassier

1 https://projects.cs.dal.ca/projectx/

2 Attack payloads that introduce no foreign code, but control the flow of execution in a target process by leaping around memory that has already been mapped as executable, in an unanticipated fashion.

1998 – 2003	BA with honours in Contemporary Studies and Spanish Dalhousie University, Halifax, Nova Scotia Thesis: *Clockwork of the Soul: The Infrastructure of the Sign in Bergson and Artaud* Supervisor: Prof. Jure Gantar

OTHER TRAINING

Jun., '23	Practical Baseband Exploitation with Pedro Ribeiro at Recon Montreal, 2023.
Nov., '16	Corelan Advanced workshop on Windows heap exploitation techniques (heap spraying, return-oriented programming, and exploiting use-after-free vulnerabilities), with Peter van Eeckhoute, Quebec City, Hackfest '16.

PUBLICATIONS AND PRESENTATIONS (COMPUTER SCIENCE)

'A Backdoor Lockpick', talk given at *Recon Montreal*, Montreal, QC, June 9th, 2023.

'A Backdoor Lockpick: Analysing the Loopholes in Phicomm's Backdoor Protocol', talk given at *AtlSecCon '22*, Halifax, NS, April 8th, 2022.

'Return Oriented Programme Evolution with ROPER', talk given at *AtlSecCon '17*, Halifax, NS, April 28th, 2017.

'Return Oriented Programme Evolution with ROPER: A Proof of Concept', with Malcolm Heywood, Nur Zincir-Heywood, & John T. Jacobs, *Proceedings of GECCO '17 Companion, Berlin, Germany, July 15-19, 2017.*

TEACHING EXPERIENCE (COMPUTER SCIENCE & LOGIC)

CSCI 2121: *Computer Organisation & Architecture with Assembly*. With Prof. Nauzer Kalyaniwalla. Dalhousie University, Department of Computer Science. Fall, 2015 and Winter 2016. The labs I directed for this course work through most of the nand2tetris curriculum (`nand2tetris.org`), showing how a simple virtual computer can be built, iteratively, from nand gates to a working CPU, which the students implement, and then write assembly code for. The labs then cover x86 assembly, and culminate in showing the students how to "smash the stack" to execute shellcode.

PHIL 2110: *Elementary Symbolic Logic*. With Prof. Mark McCullagh. University of Guelph, Department of Philosophy. Winter, 2011. Essentially the same material as is taught in discrete mathematics courses, but sprung on unsuspecting philosophy kids.

PHIL 2130: *Logic* (*Deduction*). With Profs. Peter Schotch & A. Robinson. Philosophy. Fall/Winter, 2007-2008.

TEACHING EXPERIENCE (PHILOSOPHY & HUMANITIES)

CTMP 2203 / HSTC 2206: *Biopolitics: From Hormones to War Drones*. University of King's College, Halifax, Departments of Contemporary Studies and the History of Science and Technology. Fall, 2014.

PHIL 3180: *The Naturalization of Phenomenology in Philosophy of Mind*. University of Guelph, Department of Philosophy. Fall, 2010.

CTMP 2203 / HSTC 2206: *Biopolitics*. University of King's College, Halifax, Departments of Contemporary Studies and the History of Science and Technology. Winter, 2008.

I have about ten years of experience as a teaching assistant in various liberal arts departments, where I would regularly conduct seminars on topics including the history of science and

technology, philosophy of mind, existentialism, and death. During this time, I worked at four different universities (University of King's College, Dalhousie, Brock, and the University of Guelph), with consistently glowing student reviews. (If details are wanted, I have a separate academic CV, available upon request.)

PUBLICATIONS, PRESENTATIONS, AND TRANSLATIONS (PHILOSOPHY)

'Formalization', 'Forcing', 'Generic', 'Ideology', 'Model' and 'Suture'. In Steve Corcoran (ed.), *Badiou Dictionary*. Edinburgh: Edinburgh University Press, forthcoming.

'New Directions.' In Tristan Palmer et al. (eds.), *Badiou: Key Concepts*. Dublin: Acumen Press, 2010.

'Translator's Introduction.' In Alain Badiou. *The Concept of Model*. Trans. Z.L. Fraser. Melbourne: re.press, 2007. above entries

'The Law of the Subject: Alain Badiou, Luitzen Brouwer and the Kripkean Analyses of Forcing and the Heyting Calculus.' In Ashton, Bartlett & Clemens (eds.) *The Praxis of Alain Badiou*. Melbourne: re.press, 2006. Ch. 3: 23–70.

'The Law of the Subject: Alain Badiou, Luitzen Brouwer and the Kripkean Analyses of Forcing and the Heyting Calculus.' *Cosmos & History*. Vol. I. Issue 3. 2006: 94–133.

'Discourse on the Phenomenal Text and the Nature of Babylonian Divination.' *Tooth & Claw: Journal of the King's History of Science Society*. Vol. I. No. 1 (2003): 28–46.

Fernando Zalamea, *Synthetic Philosophy of Contemporary Mathematics*. Falmouth & New York: Urbanomic & Sequence Press, 2013. Translation of *Filosofía sintética de las matemáticas contemporáneas*. Bogota: Universidad Nacional de Colombia, 2009.

Alain Badiou, *The Concept of Model: Introduction to the Materialist Epistemology of Mathematics*, Melbourne: re.press, 2007. Translation of Le concept de modèle: introduction a l'épistémologie materialiste des mathématiques. Paris: François Maspero, 1969.

I have also translated about half a dozen articles, which haven't been listed here. A complete list is available upon request.

EVENTS ORGANIZED

Formalisation & Dialectics: Form & Formalism III. Conference held at Jan van Eyck Academie, Maastricht. June 7–8, 2012.

Versus Laboratory. Seminar series conducted at Jan van Eyck Academie, Maastricht, between September, 2011 and February, 2012. Guest speakers included Fernando Zalamea (Colombia), Katerina Kolozova (Macedonia), and Ray Brassier (Lebanon).

Logic seminar. Seminar series conducted at Jan van Eyck Academie, Maastricht, between November, 2011 and November, 2012, in which I introduced topics in mathematical logic to a non-mathematical audience.

RECENT TALKS, WORKSHOPS, AND CONFERENCE PRESENTATIONS[3]

A Question of Will, pt. 2, Bratislava, Slovakia, Jan. 28, 2017.

Artificial Intelligence in the Age of Sexual Reproduction, hosted by Glass Bead, Les Laboratoires d'Aubervilliers, Paris, Sept. 29, 2014.

Go back to An-Fang, lecture on Hegel's dialectics and Jean-Yves Girard's work in mathematical logic, delivered at *Formalisation & Dialectic: Form & Formalism III*, June 8, 2012, at the Jan van Eyck Academie, Maastricht.

3 A full list is available upon request.

Logics of Sonification & Sonifications of Logic, full-day workshop conducted with Julian Rohrhuber at Institut fuer Musiek und Medien, Robert Schumann Hochschule, Dusseldorf, Germany, on November 20, 2012. Abstract available at http://alturl.com/3uyfw

Éclats de la dialectique dans les courts-circuits de la syntaxe: Hegel, Miller, Petersen, et Girard, seminar conducted as part of the series 'Formalisme(s): la philosophie française et les sciences formelles', at L'École Normale Superieure, Paris, France on February 22, 2012. Abstract available at http://www.ciepfc.fr/spip.php?article274

Seminario 1: Sobre El Concepto de Modelo *de Alain Badiou, y el Teorema de Löwenheim-Skolem: Le brecha entre la Semantica y el Sintaxis como espacio para invención y perturbación y no como la superficie de un espejo*, Department of Mathematics and Physics, Universided Iberoamericana, Mexico City, May 10, 2011.

Seminario 2: El Concepto y la Categoria de Forcing, desde 'La subversion infinitesimal' hasta El Ser y el Acontecimiento, Department of Mathematics and Physics, Universided Iberoamericana, Mexico City, May 11, 2011.

Seminario 3: El Proyecto lógico de Jean-Yves Girard, como radicalización de ciertos temas ya considerados, y como condición contemporánea para la filosofía, Department of Mathematics and Physics, Universided Iberoamericana, Mexico City, May 11, 2011.

April 25, 2023