Lesly-Ann Daniel

Postdoctoral researcher,
Interested in formal methods for software & hardware security

Distributed and Secure Software (DistriNet)
Celestijnenlaan 200A - box 2402
3001 Leuven, Belgium
+33 (658893819)
lesly-ann.daniel@kuleuven.fr
leslyann-daniel.fr

Education

2018–2021 **PhD, Computer Science**, Université Côte d'Azur, France.

2016–2018 **Master, Computer Science**, *with highest honour*, University of Rennes 1, France.

2016–2018 **Magistère, Computer Science**, ENS Rennes, France.
Training focused on research through lectures, seminars, visits of labs, etc.

2013–2016 **Bachelor, Computer Science**, *with highest honour*, University of Limoges, France.

Research Results

I am interested in the application of formal methods for software and hardware security. In particular, I have worked on automatic verification of cryptographic implementations in order to check the absence of microarchitectural and Spectre attacks.

Research projects

Efficient symbolic analysis for constant-time and secret-erasure at binary level
- Optimizations for relational symbolic execution at binary level yielding dramatic improvement over prior approaches
- Formal proof: correctness of the analysis for bug-finding and bounded verification
- Framework to check constant-time and secret-erasure preservation in multiple compiler setups

Efficient symbolic analysis for detecting vulnerabilities to Spectre attacks
- Model processor speculations in symbolic execution + dedicated optimizations to reduce state explosion
- Formal proof: our optimized analysis is functionally equivalent to an unoptimized analysis

Practical impact

For these projects, I developed **two open-source tools** which lead me to the following interesting findings:
- Backend passes of `clang` can introduce constant-time violations out-of-reach of llvm analyses
- Contrary to `clang`, `gcc` optimizations (in particular the if-conversion) help preserve constant-time
- Volatile function pointers can introduce additional register spilling that might break secret-erasure
- Index-masking, a standard defense against Spectre-PHT, may be bypassed with Spectre-STL
- Position-independent-code may introduce Spectre violations

Papers and talks

- I am the author of **5 publications**, including 2 publications top-tier security conferences, **SP'20** and **NDSS'21**
- I presented my research in more than **10 talks**

Research Experience

Oct 2022–2024 **Postdoc: Design of Hardware Extensions for Security**, *DistriNet, KU Leuven*, Belgium,
Under the supervision of Frank Piessens.
Formal design of hardware extensions for security, such as hardware mitigations for secure speculation.

Sept 2019–Nov 2019 **Visiting researcher at Information Science Institute (ISI)**, *University of Southern California (USC)*, California, United-States.
Work with Christophe Hauser on symbolic verification for cryptographic primitives.

Oct 2018–Oct 2021 **PhD: Symbolic Binary-Level Code Analysis for Security**, *CEA List, Univ. Côte d'Azur, Inria*, France,
Under the supervision of Sébastien Bardin and Tamara Rezk.
Design of efficient symbolic analyzes for information flow properties at binary-level, with applications to cryptographic constant-time, secret-erasure and detections of Spectre vulnerabilities.

Feb 2018–Aug 2018 **Internship: Bug-Finding, from Safety to Hypersafety**, *CEA List*, France,
Under the supervision of Sébastien Bardin.
Adaptation of symbolic execution for bug-finding of information-flow properties.

May 2017–Aug 2017 **Internship: Protocol State Fuzzing of OpenVPN**, *Radboud University*, The Netherlands,
Under the supervision of Eric Poll.
Design of a test harness to automatically infer a model of an OpenVPN server using LearnLib.

Jan 2016–May 2016 **Project: Native Mutant Generator**, *University of Limoges*, France,
Under the supervision of Jean-Louis Lanet.
Implementation of an ARM disassembler and an API to mutate specific instructions or sections while preserving the ELF format, in the context of fault-injection research.

Awards and Grants

Sept 2020 **Award: L'Oréal-UNESCO Young Talents France for Women in Science**,
Award for my work on automated program analysis for security (15000€).

Sept 2018 **Fellowship: Phare-CEA**, Grant for a 3 year PhD.

Software

The tools I developed and their experimental evaluation are all *open-source* on github.

Binsec/Rel: Binary-level symbolic analyzer for cryptographic constant-time & secret-erasure. Experimental evaluation on 308 cryprographic binaries.
Available at: `https://github.com/binsec/rel` and `https://github.com/binsec/rel_bench`

Binsec/Haunted: Binary analyzer to detect Spectre-PHT and Spectre-STL vulnerabilities. Experimental evaluation on small test cases and 5 cryptographic primitives.
Available at: `https://github.com/binsec/haunted` and `https://github.com/binsec/haunted_bench`

Properties vs. compilers: Easily extensible frameworks to check the preservation of constant-time and secret-erasure for multiple small programs, compiled with multiple compilers and options. Application: analysis of a total of 2006 binaries for constant-time and 1156 binaries for secret-erasure.
Available at: `https://github.com/binsec/rel_bench/tree/main/properties_vs_compilers`

Spectre-STL litmus tests: A set of small test cases for Spectre-STL which has been reused by the community.
Available at: `https://github.com/binsec/haunted_bench/blob/master/src/litmus-stl/programs/spectrev4.c`

Teaching and student supervision

July–Sep 2021 **Internship supervision of a 1st year Master student**.
Topic: Optimizing Relational Symbolic Execution Over Cryptographic Code.

Apr–Jun 2020 **Computer Architecture**, *IUT Orsay*, France, Tutorial 24h.

Nov–Jan 2020 **Operating Systems**, *ENSTA*, France, Tutorial 15h.

Jan–Mar 2019 **Compilation**, *IUT Orsay*, France, Tutorial 16h + Preparation and correction of practical exam.

Oct–Dec 2018 **C programming**, *ENSTA*, France, Tutorial 16h + Correction of written exam.

2015–2016 **Mentoring in Computer Science**, *University of Limoges*, France, Helping 1st year B.S. students in CS.

Academic service

Reviewer Peerj 2020 (journal)

PC CAV'22 (Artifact committee), PLDI'21 (Artifact committee), ACSAC'20 (Artifact committee)

Session chair ACSAC'20

Sub-reviewer DIMVA'21, BAR'21, SecDev'20, ACSAC'20, BAR'20

Peer Reviewed Publications

Conference

Hunting the Haunter: Efficient Relational Symbolic Execution for Spectre with Haunted RelSE, *L. Daniel, S. Bardin, T. Rezk*, Network and Distributed System Security Symposium (NDSS), 2021. Core rank: **A***.

Binsec/Rel: Efficient Relational Symbolic Execution for Constant-Time at Binary-Level, *L. Daniel, S. Bardin, T. Rezk*, IEEE Symposium on Security and Privacy (SP), 2020. Core rank: **A***.

Workshop

[To appear] **Reflections on the Experimental Evaluation of a Binary-Level Symbolic Analyzer for Spectre**, *L. Daniel, S. Bardin, T. Rezk*, Workshop postproceedings, Learning from Authoritative Security Experiment Results (LASER), 2022.

Inferring OpenVPN State Machines Using Protocol State Fuzzing, *L. Daniel, J. de Ruiter, E. Poll*, Workshop on Security Protocol Implementations: Development and Analysis (SPIDA), 2018.

Thesis

Symbolic Binary-Level Code Analysis for Security, *L. Daniel*, PhD thesis, Université Côte d'Azur, 2021.

Journal submission

[Under revision] **Binsec/Rel: Symbolic Binary Analyzer for Security with Applications to Constant-Time and Secret-Erasure**, *L. Daniel, S. Bardin, T. Rezk*, ACM Transactions on Privacy and Security (TOPS), 2021.

List of Talks

Invited talks

May, 2022 [Incoming] **Symbolic Binary-Level Code Analysis for Security**, Invited talk at Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI) to present my PhD defense (France).

Mar 16 2021 **Efficient Relational Symbolic Execution for Speculative Constant-Time at Binary-Level**, Invited talk at the annual meeting of the french research group on formal methods for computer security (online).

Feb 25 2021 **Experimental Evaluation of a Binary-Level Symbolic Analyzer for Spectre: Binsec/Haunted**, Invited talk about our experimental work at LASER'21 workshop, colocated with NDSS'21 (online).

Conference talks

Feb 23 2021 **Hunting the Haunter: Efficient Relational Symbolic Execution for Spectre with Haunted RelSE**, Paper presentation at NDSS (online).

May 19 2020 **Binsec/Rel: Efficient Relational Symbolic Execution for Constant-Time at Binary-Level**, Paper presentation at SP (online).

Apr 23 2018 **Inferring OpenVPN State Machines Using Protocol State Fuzzing**, Paper presentation at SPIDA (London, United-Kingdom).

Technical talks and seminars

Nov 12 2021 **Symbolic Binary-Level Code Analysis for Security**, *L. Daniel*, PhD defense, Inria (Saclay, France).

Oct 25 2021 **Symbolic Binary-Level Code Analysis for Speculative Constant-Time**, Technical talk for TEE Group Tech Talk Series, KU Leuven (Leuven, Belgium).

Feb 8 2021 **Efficient Relational Symbolic Execution for Speculative Constant-Time at Binary-Level**, Student talk at *Cyber in Saclay*, Winter School on Cybersecurity (online).

Dec 7 2019 **Binsec, A Binary Analysis Platform**, Lightning talk at Blackhoodie (Vienna, Austria).

Nov 12 2019 **Binsec/Rel: Efficient Constant-Time Analysis of Binary-Level Code with Relational Symbolic Execution**, Security seminar UCSD (San-Diego, CA, United-States).

Nov 5 2019 **Binsec/Rel: Efficient Constant-Time Analysis of Binary-Level Code with Relational Symbolic Execution**, ISI Cybersecurity Seminar (Los Angeles, CA, United-States).

Popularization

I like sharing my research to a wider audience, especially with the hope to encourage young girls to get an interest in computer science.

Dec-Jan 2022 **Mentor at *For Girls in Science, Scientific Challenge***, France.
Mentoring high school student for a scientific project, as part of a program to promote science to young girls.

22nd Nov 2020 **Verification in Computer Science**, *with Myriam Clouet*, Talk at *Rendez-vous des jeunes mathématiciennes et informaticiennes (RJMI)*, France.
Presentation of our background and thesis to young female high school students.

Nov 2020 **Time, a critical notion in software development**, *with Sébastien Bardin, Virgile Prévosto, Julien Signoles, Patrick Tessier*, Press article in *Clefs CEA*.
Presentation of timing attacks and constant-time programming for cryptography to a nonspecialist audience.

June 27 2019 **Formal methods, but what is that?**, *with Florent Chevrou*, Talk at festival PSES 2019, France.
Overview of secure design and software verification for an audience of developers unfamiliar with formal methods.