Lesly-Ann Daniel

PhD student interested in formal methods for security

7 dom. de la butte à la reine
91120 Palaiseau
France
+33 (658893819)
✉ lesly-ann.daniel@ens-rennes.fr
leslyann-daniel.fr

Experience

2018–2021 **PhD—Software Security, from Safety to Hypersafety**, *CEA List*, France,
Under the supervision of Sébastien Bardin and Tamara Rezk.
During my PhD I worked on efficient bug-finding and bounded-verification of information flow properties at binary-level, with applications to cryptographic constant-time, secret-erasure and vulnerabilities to Spectre attacks.

Feb 2018– Aug 2018 **Internship—Software Security, from Safety to Hypersafety**, *CEA List*, France,
Under the supervision of Sébastien Bardin.
Adapt 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.
Build 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.
Build an ARM disassembler and an API to smartly mutate specific binary sections or instructions.

Awards

Sept 2020 **Fellowship L'Oréal-UNESCO Young Talents France for Women in Science**.
For my work on automated program analysis for security.

Collaborations

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

Education

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

2016–2018 **Master, Computer science,** with a focus on software security, *University of Rennes 1*, France.

2013–2016 **Bachelor, Computer science**, *University of Limoges*, France.

Publications

2021 **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).

2020 **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).

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

Tools

Binsec/Haunted, *Binary analyzer to detect Spectre-PHT and Spectre-STL vulnerabilities*.
`https://github.com/binsec/haunted`

Binsec/Rel, *Symbolic analyzer for cryptographic constant-time verification at binary-level*.
`https://github.com/binsec/rel`

Talks

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

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

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

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

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

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

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

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

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

Teaching

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 & Writing 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.

Popularization

I like giving popularization talks, especially with the hope to encourage young girls to get an interest in computer science.

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.

27th June 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.

Academic service

Reviewer	Peerj 2020 (journal)	Session chair	ACSAC'20
PC	PLDI'21 (Artifact committee), ACSAC'20 (Artifact committee)	Sub-reviewer	DIMVA'21, BAR'21, SecDev'20, ACSAC'20, BAR'20

Others

Languages

French	Native language
English	Full working proficiency (TOEIC: 955)

Interests

I also like climbing, running, hiking, reading, playing the guitar, and knitting.

Voluntary Work

You can find me every first Saturday of the month at the install party of *Premier Samedi du Libre* at *Carrefour Numérique de la Cité de Sciences*, Paris, helping people installing *free software*.