ACADEMIC CURRICULUM VITAE – LUCCA HIRSCHI

PERSONAL INFORMATION

Lucca Hirschi (Dr.)
ETH Zürich
Universitätstrasse 6
8092 Zürich
lucca.hirschi@ens-lyon.org
https://www.inf.ethz.ch/personal/lhirschi/

I am a postdoctoral researcher at ETH Zürich in Prof. David Basin's *Information Security Group*. My research interests mainly focus on *formal methods* for *security* and *privacy*. I design new verification techniques, algorithms and tools to effectively and efficiently analyze formal security properties. I generally enjoy research projects that combine both theoretical contributions and practical applications.

EMPLOYMENT

(06/2017-) — **Postdoc researcher & teaching assistant** at ETH Zürich in Prof. David Basin's *Information Security Group*.

(09/2013-05/2017) — **Ph.D student & teaching assistant** at LSV, Ecole Normale Supérieure de Cachan.

EDUCATION

(09/2013-05/2017) — **Ph.D** at LSV, Ecole Normale Supérieure de Cachan under the supervision of Stéphanie Delaune and David Baelde. Thesis title : *Automated Verification of Privacy in Security Protocols : Back and Forth Between Theory & Practice*.

(09/2010-09/2013) — **Bachelor & Master of Science Degree in Theoretical Computer Science** at Ecole Normale Supérieure de Lyon (university level institution training teachers and researchers, entrance to which is based on a competitive exam), Lyon, France.

(09/2008-09/2010) — **Classes préparatoires scientifiques** at Lycée du Parc (post-secondary preparatory classes in science for competitive entrance exams), Lyon, France.

PUBLICATIONS IN INTERNATIONAL PEER-REVIEWED JOURNALS

D. Baelde, S. Delaune and L. Hirschi. *A Reduced Semantics for Deciding Trace Equivalence.* In journal of **Logical Methods in Computer Science** 13, issue 2. Episciences, 2017.

S. Delaune and L. Hirschi. *A survey of symbolic methods for establishing equivalence-based properties in cryptographic protocols.* In journal of **Logic and Algebraic Programming** 87, pages 127-144. Elsevier, 2016.

PUBLICATIONS IN INTERNATIONAL PEER-REVIEWED CONFERENCES

A. Doumane, D. Baelde, L. Hirschi and A. Saurin. *Towards Completeness via Proof Search in the Linear Time μ-calculus.* In **LICS'16**, pages 377-386. ACM Press, 2016.

L. Hirschi, D. Baelde and S. Delaune. *A method for verifying privacy-type properties : the unbounded case.* In **S&P'16**, pages 564-581. IEEECSP, 2016

D. Baelde, S. Delaune and L. Hirschi. *Partial Order Reduction for Security Protocols.* In **CONCUR'15**, Leibniz International Proceedings in Informatics 42, pages 497-510. Leibniz-Zentrum für Informatik, 2015.

D. Baelde, S. Delaune and L. Hirschi. *A reduced semantics for deciding trace equivalence*

using constraint systems. In **POST'14**, LNCS 8414, pages 1-21. Springer, 2014.

Publications in International Peer-Reviewed Workshops

Piers O'Hanlon, Ravishankar Borgaonkar and Lucca Hirschi. *Mobile subscriber WiFi privacy.* Accepted at **MoST'17** (S&P Workshops) (**best paper award**). 2017.

Works not yet published

D. Baelde and S. Delaune, L. Hirschi *POR for Security Protocol Equivalences : Beyond Action-Determinism.* Under submission at CAV 2018.

Jannik Dreier, Lucca Hirschi, Saša Radomirovic and Ralf Sasse. *Automated Unbounded Verification of Stateful Cryptographic Protocols with Exclusive OR Operations.* Under submission at CSF 2018.

L. Hirschi, D. Baelde and S. Delaune. *A method for unbounded verification of privacy-type properties.* Under submission at Journal of Computer Security.

C. Cremers and L. Hirschi. *Improving Automatic Symbolic Analysis for E-voting Protocols : Sufficient Conditions for Ballot Secrecy.* Soon to be submitted.

R. Borgaonkar, L. Hirschi, A. Martin, S. Park, J.-P. Seifert and A. Shaik. *New Privacy Threat on 3G, 4G and incoming 5G AKA Protocol.* Soon to be submitted. Associated proposal of briefing accepted at **Black Hat USA'17**.

Invited talks

2017 — **Invited talk** at the conference **Troopers'17** (shared with R. Borgaonkar) about our *New Privacy Threat on 3G, 4G and incoming 5G AKA Protocol* paper.
— **Invited talk** at **GSMA Fraud & Security** meeting presenting the same work.
2015 — **Invited talk** at NII Shonan Meeting 069 - Logic and Verification Methods in Security and Privacy (Dagstuhl-like Seminars in Japan).

Grants, Prizes, Competitive Selections

2018 — **Pre-selected** to be interviewed for a **tenured scientist position at CNRS**.
2017 — Our proposition of briefing about our *New Privacy Threat on 3G, 4G and incoming 5G AKA Protocol* paper has been accepted at **Black Hat USA'17**.
— **Best paper award** at MoST'17 for our *Mobile subscriber WiFi privacy* paper.
2016 — **European COST Grant** by European Cooperation in Science and Technology (Crypto Action) and **mobility grant from the Doctoral School Paris-Saclay** for visiting Professor Cas Cremers at University of Oxford (3 month academic visit).

Student Supervisions

2017 — David Lanzenberger (bachelor student at ETH Zürich) : Formal Analysis of 5G Protocols (co-supervision).
— Vincent Stettler (master student at ETH Zürich) : NextGen Network Security Analysis (co-supervision).

Industrial Relevance & Media Coverage

Our work *New Privacy Threat on 3G, 4G and incoming 5G AKA Protocol* has been presented at **Black Hat USA'17**. We also presented those attacks directly to the **GSMA consortium** where most of the worldwide 4G operators are members as well as to the **3GPP** responsible of mobile communication standardization. Our findings also got some press coverage : ZDnet (and Zero Day), Forbes, The Register, International Business Times, Silicon.de.

We started mid 2017 a 1 year project (100'000 CHF) between ETH Zürich (David Basin, Ralf Sasse and me) and Huawei Technologies Singapore Research Center. This project

involves a bilateral collaboration on NextGen telecommunication security protocols (we analyze Huawei design proposals, they share their case studies) and an industrial transfer : Ralf Sasse and I went to Singapore to give a 4 days in-depth tutorial on the (academic) tool Tamarin (automatic prover of formal security guarantees) for a dozen of Huawei engineers. We thus both promote formal methods in the industrial sector and make available verification techniques to engineers that will notably be responsible of the standardization and implementation of many security protocols, e.g., in the 5G ecosystem.

TOOLS & SOFTWARE

UKano — Automatic verifier of unlinkability and anonymity for a large class of 2-agents protocols (in OCaml, $\approx$ 2 kloc). Notably used to discover new attacks on ePassport protocols. Open-source, available on Github and at https://projects.lsv.ens-cachan.fr/ukano/.
POR for APTE — Implementation of Partial Order Reduction techniques in the tool APTE which considerably improved its practical impact (in OCaml, $\approx$ 3 kloc). Open-source, available on Github and at http://www.lsv.fr/~hirschi/apte_por. Implementation of similar techniques in the tool SPEC (in Bedwyr, $\approx$ 3.3 kloc).

SERVICE & PROJECTS

I have reviewed papers for CSF, Euro S&P, CCS, POST (ETAPS), the Journal of Computer Security and the journal LNCS Transactions on Petri Nets and Other Models of Concurrency.
Participation to projects : joint project between Huawei Technologies Singapore Research Center and ETH Zürich on 5G protocols, ERC Starting Grant POPSTAR, ANR project Sequoia, ANR project ProSe, ANR JCJC project VIP.

VISITING & INTERNSHIPS

2016 — 3 month-academic visit at University of Oxford with Professor Cas Cremers. The two collaborations started there with respectively Cas Cremers and Ravishankar Borgaonkar resulted in a briefing at **Black Hat USA'17**, a paper published at **MoST'17**, and two papers under submission.
2013 — 4 month internship about reduction of interleavings for trace equivalence checking of security protocols with David Baelde & Stéphanie Delaune, LSV, ENS Cachan.
2012 — 3 month internship about infinite and cyclic proofs and Büchi automata directed by David Baelde, PLS lab, IT University of Copenhagen, Denmerk. Work continued later on with Amina Doumane and Alexis Saurin, leading to a publication at **LICS'16**.
— 2 month internship about alternating automata for XPath queries directed by Kim Nguyên, LRI lab, Paris-Sud.
2011 — 6 week internship about type-safe language for XML directed by Giuseppe Castagna and Kim Nguyên, PPS lab, Paris-7.

TEACHING ACTIVITIES

2018 (30h) — Information Security at ETH Zürich (lab classes).
2017 (30h) — Numerical Methods for CSE at ETH Zürich (lab classes).
(20h) — Tutorial on the Tamarin prover given at Huawei Technologies Singapore Research Center.
2013-2017 — Teaching assistant at ENS Cachan :
($2*45+12$h) — Computer Programming : C, OCaml, compiler project (lab classes).
($2*22.5$h) — Logic (tutorial classes).
(30h) — Software engineering (project).
($2*11$h) — Introduction to the Coq Proof Assistant (lab classes).
(22.5h) — Projects around Logic : SAT and Coq.
(22.5h) — Computability (tutorial classes).

VULGARIZATION

2013 — Hosted a one day workshop for secondary school pupils on cryptography at the Science Fair (Fête de la science) 2013.

PARTICIPATION TO CONFERENCES & SCHOOLS

Conferences — Troopers'17, S&P'16 (Oakland), POST'16 (ETAPS), CONCUR'15, CSF'15, POST'15, JFLA'15, LICS&CSF'15 (VSL), POST'14 (ETAPS).

Schools — EPIT'15 (École « Preuve mécanisée de programmes »),
— The Joint EasyCrypt-F*-CryptoVerif School (2014),
— 13th & 14th International School on Foundations of Security Analysis and Design (2013 & 2014).

Workshops — Logic and Verification Methods in Security and Privacy (NII Shonan Meeting Seminar) (2015), Workshop on Abella and Bedwyr at LIX (2012).

TECHNICAL SKILLS

OCaml, Python, C, C++, Haskell, assembly (x86, mips). Knowledge in logic programming.

ADMINISTRATIVE TASKS

I am organizing the internal seminar of the Information Security group at ETH Zürich (2018-). I was organizing the monthly internal seminar of my group at LSV, ENS Cachan (2015-2017). I helped organizing the Workshop on the 20th Anniversary of LSV (2017). I helped organizing the Colloquium in honour of Martin Abadi (2015).