Kirill Nikitin

Curriculum Vitae
EPFL IC IINFCOM DEDIS, BC 209,
Station 14, CH-1015 Lausanne, Switzerland
mob. +47 77 9866320
kirill.nikitin@epfl.ch
https://nikirill.com

EDUCATION

Ph.D. Computer and Communication Sciences 2015-now

Decentralized and Distributed Systems Lab, École polytechnique fédérale de Lausanne, Switzerland

Future thesis:"Exploiting and Protecting Metadata in Encrypted Files and Communications"
Thesis advisor: Bryan Ford

M.S. Communication Systems 2013-2015

KTH Royal Institute of Technology, Stockholm, Sweden

Thesis: "DTLS Adaptation for Efficient Secure Group Communication" @ RISE SICS
Advisors: Marco Tiloca, Shahid Raza (both RISE SICS), Markus Hidell (KTH)

Specialist Degree Information Security (with honors) 2008-2013

Kazan (Volga Region) Federal University, Russia

Thesis: "Cryptographic Key Distribution via Randomness from Multipath Propagation of Radio Waves"
Advisor: Arkady Karpov

Exchange Student Computer Science 2012

University of Helsinki, Finland

PEER-REVIEWED PUBLICATIONS [Google Scholar ID]

4. J. Lee, K. Nikitin, S. Setty. "Replicated state machines without replicated execution". In *IEEE Symposium on Security and Privacy*, 2020.

3. K. Nikitin, L. Barman, W. Lueks, M. Underwood, J.-P. Hubaux, B. Ford. "Reducing Metadata Leakage from Encrypted Files and Communication with PURBs". In *Privacy Enhancing Technologies Symposium*, 2019.

2. K. Nikitin, E. Kokoris-Kogias, P. Jovanovic, N. Gailly, L. Gasser, I. Khoffi, J. Cappos, and B. Ford. "CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds". In *USENIX Security Symposium*, 2017.

1. M. Tiloca, K. Nikitin, S. Raza. "Axiom: DTLS-Based Secure IoT Group Communication". In *ACM Transactions on Embedded Computing Systems (TECS), Special Issue on Embedded Computing for IoT, 16(3), 66*, April 2017.

PROFESSIONAL EXPERIENCE

Doctoral Researcher Sept 2015–now
Decentralized and Distributed Systems lab, **EPFL**, Lausanne, Switzerland
The lead of the research projects on:

- Exploitng and protecting metadata in encrypted files and communications;
- Security and transparency of software-distribution systems.

Research Intern Aug–Oct 2019
Confidential Computing Group, **Microsoft Research**, Cambridge, UK

- Information-flow control for confidentiality in smart contracts.

Research Intern Aug–Nov 2018
Systems Security and Privacy Group, **Microsoft Research**, Redmond, US

- Improving scalability of smart contracts via off-chain execution and verifiable computation.

External Master's Thesis Jan–Jun 2015
Security Lab, **RISE Swedish Institute of Computer Science**, Stockholm, Sweden

- Designing a protocol for secure group communication for the Internet-of-Things.

Research Intern Jun–Aug 2014
Laboratory for Cryptologic Algorithms, **EPFL**, Lausanne, Switzerland

- Integer factorization and analysis of public-key ecosystem weaknesses.

ACADEMIC SERVICE AND EXTRACURRICULAR ACTIVITIES

- Program Committee member at
  - CryBlock 2019, 2020: Workshop on Cryptocurrencies and Blockchains for Distributed Systems.
  - BlockSys 2019: Workshop on Blockchain-enabled Networked Sensor Systems
  - ICBC 2019: IEEE International Conference on Blockchain and Cryptocurrency

- An external reviewer for IEEE Tran. on Industrial Informatics 2019 and IEEE Tran. on Parallel and Distributed Systems 2020 and a sub-reviewer for ACM Conf. on Computer and Communications Security 2017.

- I was a president of a graduate student association at IC EPFL. Organized invited talks, activities for current students, and helped with the organization of Open Houses for newcomers.

- Back in the past, I played in a student theater, performing team comedy stand-ups.

TEACHING AND SUPERVISION

- **ICC Information, Computation and Communication** (Spring 20)
  Guided students during exercise solving.
- **CS-234 Technologies of societal self-organization** (Fall 19)
  Participated in the design of the brand-new course: guiding projects and creating assignments, quizzes, and the exam.

- **CS-438 Decentralized Systems Engineering** (Fall 17, 18)
  As a part of a team, designed, implemented and graded homework assignments, supervised semester group projects, and evaluated student progress throughout semester.
- **COM-402 Information Security and Privacy** (Spring 17, 18)
  As a part of a team, designed and implemented CTF-style exercise labs from scratch,contributed to creating lectures and guided students. *Student reviews:*
  "Best homeworks I've ever had at EPFL so far. They are neither too guided or to free just perfect..." "Exercises are really interesting..." "Homeworks are awesome." "Oscillating between "These exercises are insuffurable!" (before you get your token...) and "These exercises are so fun!" (after you get your token!) ..." "The Excercises are not always easy, but they are fun to do and give a good practical insight into security."
- **MATH-101 Analyse I** (Fall 16)
  Guided students during exercise solving.
- **COM-102 Advanced information, computation, communication II** (Spring 16)
  Designed exercises on basic cryptography (part of the course) and guided students.

Supervision:

- Fernando Monje Real. "Traffic analysis of real-time collaborative editors". *Master's thesis* (Spring 20).
- Carlos Villa Sánchez. "Secure management of browser extensions and their dependencies". *Master's thesis* (Spring 20).
- Charles Parzy-Turlat. "Tree-based Group Key Agreement". *Master's project* (Spring 19).
- Simone Colombo. "DecenArch: a decentralized system for privacy-conscious Web archiving against censorship". *Master's thesis* (Spring 18).
- Nicolas Plancherel. "Decentralized Internet Archive". *Master's thesis* (Fall 17).
- Nicolas Ritter. "Access Control In Real-Time Peer-to-Peer Collaboration". *Master's project* (Fall 17).
- Damien Aymon. "Implementation of an Algorithm for Peer-to-Peer Collaborative Editing". *Bachelor's project* (Spring 17).
- Rehan Mulakhel. "Web Interface for Secure Decentralized Collaboration Platform". *Bachelor's project* (Spring 17).
- Gaspard Zoss. "Enhancing Debian Update Service". *Master's project* (Fall 17).

AWARDS

- 2020: The Swiss National Science Foundation Doc.Mobility Fellowship
- 2015: EPFL EDIC Fellowship for Doctoral Studies
- 2013-2015: The Swedish Institute Scholarship
- 2009, 2011, 2012: Triple scholar of Vladimir Potanin Fellowship Program