Kirill Nikitin

Updated: 19/04/2023

Curriculum Vitae
Bloomberg Center
2 West Loop Road, New York, NY 10044

mob. +1 929 2565684
kirill@cornell.edu
https://nikirill.com

Education

Ph.D. Computer and Communication Sciences Sep 2015–Nov 2021
École polytechnique fédérale de Lausanne, Switzerland
Thesis: "Integrity and Metadata Protection in Data Retrieval"
Advisor: Bryan Ford

M.S. Communication Systems Sep 2013–Oct 2015
KTH Royal Institute of Technology, Sweden
Thesis: "DTLS Adaptation for Efficient Secure Group Communication" @ RISE SICS
Advisors: Marco Tiloca, Shahid Raza (both RISE SICS), Markus Hidell (KTH)

Diploma Information Security (with honors) Sep 2008–Jun 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 Jan–May 2012
University of Helsinki, Finland

Refereed Publications [Google Scholar]

5. S. Colombo, K. Nikitin, B. Ford, D. Wu, H. Corrigan-Gibbs. "Authenticated private information retrieval". In *USENIX Security Symposium*, 2023 (to appear).
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". *Proceedings on Privacy Enhancing Technologies, 2019(4)*, 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*, 2017.

Reports and manuscripts:

2. C. Basescu, M. Nowlan, K. Nikitin, J. Faleiro, and B. Ford, "Crux: Locality-Preserving Distributed Services". Technical report, in *CoRR*, 1405.0637, arXiv, 2018.
1. M. Tiloca, S. Raza, K. Nikitin, and S. Kumar. "Secure Two-Way DTLS-Based Group Communication in the IoT (work in progress)". *IETF*, 2015.

Professional Experience

Post-Doctoral Researcher Mar 2022–now
Cornell Tech, **Cornell University**, New York, NY

- Protecting network metadata in online communication.

Doctoral Researcher Sep 2015–Aug 2021
Decentralized and Distributed Systems laboratory, **EPFL**, Lausanne, Switzerland

- Exploiting 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

- A member of the program committee or the student editorial board for
  - ACM CCS 2023: ACM Conference on Computer and Communications Security
  - JSys 2021: Journal of Systems Research
  - ACM CCS 2021 Posters & Demos
  - 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 Eurocrypt 2022, IEEE Transactions on Industrial Informatics 2019, IEEE Transactions on Parallel and Distributed Systems 2020, and ACM CCS 2017, 2021.
- I was a president of the graduate student association at IC EPFL. Organized invited talks, activities for current students, and helped with the organization of Open Houses for newcomers.

Teaching and Supervision

- **CS-438 Decentralized Systems Engineering** (Fall 17, 18, 20)
- **ICC Information, Computation and Communication** (Spring 20)

- **CS-234 Technologies of societal self-organization** (Fall 19)
- **COM-402 Information Security and Privacy** (Spring 17, 18)
- **MATH-101 Analyse I** (Fall 16)
- **COM-102 Advanced information, computation, communication II** (Spring 16)

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