

Nils Hendrik Lukas

318A Spruce St, Canada, ON N2L 0E9

🌐 <https://nilslukas.github.io>

✉ nlukas@uwaterloo.ca

🐙 nilslukas

☎ 226-505-1605

Research

Under Submission, 2023	-
<u>N. Lukas</u> and F. Kerschbaum, 'Pick your Poison: Undetectability versus Robustness in Data poisoning Attacks against Deep Image Classification'	May 2023
USENIX Security, 2023	Anaheim, CA
<u>N. Lukas</u> and F. Kerschbaum, 'PTW: Pivotal Tuning Watermarking for Pre-Trained Image Generators'	May 2023
The 44th IEEE Symposium on Security and Privacy, 2023	San Francisco, CA
<u>N. Lukas</u> , A. Salem, R. Sim, S. Tople, L. Wutschitz and S. Zanella-Béguelin, 'Analyzing Leakage of Personally Identifiable Information in Language Models'	Feb 2023
The 43rd IEEE Symposium on Security and Privacy, 2022	San Francisco, CA
<u>N. Lukas</u> , E. Jiang, X. Li, and F. Kerschbaum, 'SoK: How Robust is Deep Neural Network Image Classification Watermarking?'	May 2022
9th ACM Workshop on Information Hiding and Multimedia Security, 2021	Online Event
M. Shafieinejad, <u>N. Lukas</u> , J. Wang, X. Li and F. Kerschbaum, 'On the Robustness of Backdoor-based Watermarking in Deep Neural Networks'	Apr 2021
International Conference on Learning Representations (ICLR), 2021	Online Event
<u>N. Lukas</u> , Y. Zhang and F. Kerschbaum, 'Deep Neural Network Fingerprinting by Conferrable Adversarial Examples', Spotlight presentation	Jan 2021
Annual Computer Security Applications Conference (ACSAC), 2020	Online Event
R. Mahdavi, T. Humphries, B. Kacsmar, S. Krastnikov, <u>N. Lukas</u> , et al., 'Practical Over-Threshold Multi-Party Private Set Intersection'	May 2020
IEEE European Symposium on Security and Privacy, 2020	Online Event
B. Kacsmar, B. Khurram, <u>N. Lukas</u> , A. Norton, M. Shafieinejad et al., 'Differentially Private Two-Party Set Operations'	Jan 2020

EXPERIENCE

Microsoft Research	Waterloo, Canada
Research Intern on Privacy in Language Models	May 2022 - August 2022
University of Waterloo	Waterloo, Canada
Instructional Advisor for 'Object-Oriented Software Development'	since Sept 2021
University of Waterloo	Waterloo, Canada
Teaching Assistant for 'Computer Security and Privacy'	Sept 2020 - May 2021
RWTH-Aachen	Aachen, Germany
Master thesis on 'Secure Inference for Deep Neural Networks'	Feb 2018 - Aug 2018
Group on Information Systems & Database	RWTH-Aachen
Instructional Advisor for 'Data-Driven Medicine'	June 2017 - Dec 2018
MathCCES, RWTH-Aachen	Aachen, Germany
Instructional Advisor for 'Developing Interactive Web Applications'	Sept 2016 - Dec 2018

EDUCATION

University of Waterloo	Waterloo, Canada
PhD in Computer Science	since 2019
Korea University	Seoul, South Korea
Term abroad -Master of Science in Computer Science	Fall 2016
RWTH-Aachen	Aachen, Germany
Master of Science in Computer Science	2016-2018
Yonsei University	Seoul, South Korea
Term abroad - Bachelor of Science in Computer Science	Fall 2014
RWTH-Aachen	Aachen, Germany
Bachelor of Science in Computer Science	2012-2016

ADDITIONAL

- Recipient of the 2 year “David R. Cheriton Scholarship” in February 2022 [20,000 CAD]
- Student Board Member of the Cybersecurity and Privacy Institute (CPI)
- Appointed School Advisory Committee on Appointments (SACA) liaison for the CrySP lab
- Outstanding poster award by the Cybersecurity and Privacy Institute (CPI) in October 2019
- Graduation from Master’s degree with excellence in 2018
- “KU Global” scholarship for a semester abroad at Korea University in 2016
- 1st place in a hackathon on robotics hosted by Bosch, Continental and IVU
- “MOGAM” scholarship for a semester abroad at Yonsei University in 2014