Vera Rimmer

Post-Doctoral Researcher at DistriNet, KU Leuven
distrinet.cs.kuleuven.be/people/vera

ACADEMIC POSITIONS

KU LEUVEN – DISTRINET
Post-Doctoral Researcher
2023 – present | Leuven, Belgium

EDUCATION

KU LEUVEN – DISTRINET
PhD in Engineering Science: Computer Science
2022 | Leuven, Belgium

KU LEUVEN
MS in Artificial Intelligence
2016 | Leuven, Belgium

SPBPU
Specialist in Computer Security
2015 | Saint-Petersburg, Russia

INDUSTRIAL POSITIONS

PJSC RADIO TECHNOLOGIES
Programmer Analyst
Secure Software Development, Network Traffic Analysis
2012-2015 | Saint-Petersburg, Russia

PROMTRANSAUTOMATIKA
Technician Programmer
Microcontroller Programming for Safety Diagnosis in Industrial Systems
2011-2012 | Saint-Petersburg, Russia

TECHNICAL SKILLS

Languages & Frameworks
Python, Keras, C/C++, PyTorch, Tensorflow, Java, Spark, Hadoop, DL4J, bash, Javascript

Platforms
Linux (Ubuntu, Kali Linux, CentOS, Red Hat, Fedora), Mac OS, Windows

Databases
MongoDB, SQL, PL/SQL, MySQL, MS SQL Server

LINKS

LinkedIn://verarim
DistriNet://vera
Personal://verarimmer

I am a postdoc at the DistriNet lab in KU Leuven, Belgium, where I have recently completed my PhD under the supervision of Prof. Wouter Joosen and Dr. Davy Preuveneers. I research cybersecurity and privacy-enhancing technologies; applied machine learning in cybersecurity and privacy with the focus on deep learning; and trustworthiness of AI itself. My research revolves around exploring deep learning as an emerging threat against anonymous communication and around various aspects of defensive AI-enabled systems: network intrusion detection, malware detection and authentication. My experience includes three years of working in industry in the realm of software development and network security. I am genuinely interested in developing comprehensive understanding, reasonable expectations and mitigation of risks of AI applied in modern security and privacy contexts, protecting systems and individuals.

MAIN PUBLICATIONS

Dissertation: Applied Deep Learning in Security and Privacy
Doctor of Engineering Science (PhD), KU Leuven, 2022.

Trace Oddity: Methodologies for Data-Driven Traffic Analysis on Tor
V. Rimmer, T. Schnitzler, T. Van Goethem, A. Rodríguez Romero, W. Joosen, and K. Kohls
Proceedings on Privacy Enhancing Technologies (PoPETS), 2022.

Position Paper: On Advancing Adversarial Malware Generation Using Dynamic Features
A. Shafiei, V. Rimmer, I. Tsingenopoulos, L. Desmet, and W. Joosen
Proceedings of the 1st Workshop on Robust Malware Analysis (WoRMA), 2022.

Open-World Network Intrusion Detection
V. Rimmer, A. Nadeem, S. Verwer, D. Preuveneers, and W. Joosen
Security and Artificial Intelligence, Springer, 2022.

Troubleshooting an Intrusion Detection Dataset: CICIDS2017 Case Study
G. Engelen, V. Rimmer, and W. Joosen
IEEE Security and Privacy Workshops (SPW), 2021.

Automated Website Fingerprinting Through Deep Learning
V. Rimmer, D. Preuveneers, M. Juarez, T. Van Goethem, and W. Joosen
Network and Distributed System Security Symposium (NDSS), 2018.

Fishy faces: crafting adversarial images to poison face authentication
G. Garofalo, V. Rimmer, T. Van hamme, D. Preuveneers, and W. Joosen
12th USENIX Workshop on Offensive Technologies (WOOT), 2018.

Chained Anomaly Detection Models for Federated Learning: An iIntrusion Detection Case Study
D. Preuveneers, V. Rimmer, I. Tsingenopoulos, J. Spooren, W. Joosen and E. Ilie-Zudor
Applied Sciences, 2018

AWARDS

Distinguished Reviewer Award
IEEE European Symposium on Security and Privacy, 2022.

Distinguished Reviewer Award
IEEE European Symposium on Security and Privacy, 2021.

Research Forum Award
Deep Learning Security Workshop in Singapore, 2017.

TEACHING

KU LEUVEN

MSc theses supervisor
Areas:

- Intrusion Detection
- Adversarial Machine Learning
- Behavioural Authentication
- Reinforcement Learning
- Explainable AI
- Malware Detection and Analysis
- (etc.)

Teaching assistant
Computer Architecture and Software Systems
2016–2021

Teaching assistant
Object-Oriented Programming
2016–2018

SERVICE

Program co-chair

- WoRMA 2024

Program Committee member

- PETS 2024, 2023
- IEEE Euro S&P 2022, 2021, 2020
- WiSec 2023, 2022
- AISec @CCS 2023
- MLCS @ECML-PKDD 2023
- ACNS 2024
- SecTL @AsiaCCS 2023
- SECURWARE 2023
- S2RAI @SAT 2024
- WPES @CCS 2020
- NSPW 2020

(External) reviewer

- Conferences: IEEE Euro S&P 2019, PETS 2022.
- Selected Journals: Transactions on Dependable and Secure Computing, Computer Networks, IEEE Communications Magazine.

Other

- Co-Organizer of the Summer School on Security and Privacy in the Age of AI 2023.
- Mentoring Chair at IEEE Euro S&P 2023.
- Session Chair at PETS 2023.
- Posters Chair at IEEE Euro S&P 2022.
- Session Chair at IEEE Euro S&P 2022.
- Session Chair at IEEE Euro S&P 2021.
- Session Chair at IEEE Euro S&P 2020.