Daniël Vos

Updated September 20, 2023

Email: d.a.vos@tudelft.nl
GitHub: daniel-vos
LinkedIn: daniel-vos
Website: daniel-vos.github.io
Date of birth: 06-03-1998
Citizenship: Netherlands

Research interests

My research focuses on trustworthy machine learning, especially on optimizing machine learning models that are robust and that humans can understand. By leveraging combinatorial optimization techiques and novel hueristics I have trained decision tree models that resist adversarial attacks and optimized them for use in sequential decision making settings.

Education

Delft University of Technology — Delft, The Netherlands
PhD in Trustworthy Machine Learning — August 2020 – Present
Research on robust decision trees and sequential decision making
Enrolled in the research school for Information and Knowledge Systems
Expected graduation: August 2024
Promotors: Dr. S. E. Verwer and Prof. R. L. Lagendijk

Delft University of Technology — Delft, The Netherlands
MSc. Data Science — September 2018 – July 2020
Specialized in Cyber Security as part of 4TU program.
Thesis on adversarially robust decision tree learning
Supervised by Dr. S. E. Verwer.
Graduated Cum Laude *Grade average: 8.0/10*

Swiss Federal Institute of Technology — Zürich, Switzerland
Minor Computer Science — September 2017 – February 2018
Courses on: machine learning, big data, mathematical simulation and programming language design
Grade average: 5.2/6

Delft University of Technology — Delft, The Netherlands
BSc. Computer Science & Software Engineering — September 2015 – July 2018
Completed the honours programme
Graduated Cum Laude *Grade average: 8.5/10*

Publications

Differentially-Private Decision Trees with Probabilistic Robustness to Data Poisoning
Daniël Vos, Jelle Vos, Tianyu Li, Zekeriya Erkin, Sicco Verwer
Under review.

Optimal Decision Tree Policies for Markov Decision Processes
Daniël Vos and Sicco Verwer

Accepted at International Joint Conference on Artificial Intelligence, 2023.

The First AI4TSP Competition: Learning to Solve Stochastic Routing Problems
Laurens Bliek, Paulo da Costa, Reza Refaei Afshar, Robbert Reijnen, Yingqian Zhang, Tom Catshoek, Daniël Vos, Sicco Verwer, Fynn Schmitt-Ulms, André Hottung et al.
Published in Artificial Intelligence

SoK: Explainable Machine Learning for Computer Security Applications
Azqa Nadeem, Daniël Vos, Clinton Cao, Luco Pajola, Simon Dieck, Robert Baumgartner, Sicco Verwer
Accepted at European Symposium on Security and Privacy, 2023

Efficient Circuits for Permuting and Mapping Packed Values Across Leveled Homomorphic Ciphertexts
Jelle Vos, Daniël Vos, Zekeriya Erkin
Accepted at European Symposium on Research in Computer Security, 2022.

Adversarially Robust Decision Tree Relabeling
Daniël Vos and Sicco Verwer
Accepted at European Conference on Machine Learning and Principles and Practice of Knowledge Discovery in Databases, 2022.

Robust Optimal Classification Trees Against Adversarial Examples
Daniël Vos and Sicco Verwer
Accepted at AAAI Conference on Artificial Intelligence, 2022.

Efficient Training of Robust Decision Trees Against Adversarial Examples
Daniël Vos and Sicco Verwer
Accepted at International Conference on Machine Learning, 2021.

Academic Service

Reviewing
Springer Machine Learning Journal 2023
ACM Workshop on Artificial Intelligence and Security 2023
Conference on Neural Information Processing Systems 2023
AAAI Conference on Artificial Intelligence 2023
Springer Machine Learning Journal 2022

Supervising
Master thesis: *"AGONI: Adversarial Generation Of Network Intrusions"* by Wessel Thomas

Master thesis: *"Adversarial Traffic Modifications for the Network Intrusion Detection Domain"* by Maria Simidžioski
Master thesis: *"FATE: Fuzzing for Adversarial examples in Tree Ensembles"* by Cas Bilstra

Teaching experience

Teaching assistant, Cyber Security Group (TU Delft) Q4 2020 - present
CS4035: Cyber Data Analytics
Course on machine learning for cyber security, topics such as data imbalance, anomaly detection and adversarial attacks. My responsibilities include giving a lecture, creating lab work and assistance, giving demonstrations and grading.

Teaching assistant, Cyber Security Group (TU Delft) Q1 2019/2020
IN4191: Security and Cryptography
Course on the fundamentals op cryptography, topics such as (a)symmetric cryptosystems, hashes, MACs and security proofs. My responsibilities were to help students and grade their assignments.

Teaching assistant, Algorithms Group (TU Delft) Q1 2016/2017
TI1306: Reasoning and Logic
Teaching students the fundamentals of discrete mathematics, logic and proofs. I helped students and graded their weekly exercises.

Industry experience

ING Group Amsterdam, The Netherlands
Software Engineering Intern April 2018 – July 2018
For my bachelor thesis I worked in a four person team to build a web-application in which Customer Journey Experts collaboratively build diagrams. My contributions were mainly on coding the Polymer 2.0 front-end, both in developing and testing the product.

Swiss Federal Institute of Technology Zürich, Switzerland
Software Engineer / Student Researcher November 2017 – May 2018
Worked as a software engineer for the *Cocoon* research project, an effort to improve security for home IoT devices. I was supervised by Dr. Stefan Mangold. We developed an IoT node that logs internet traffic, radio spectrum and audio data to be used for analyzing smart device behavior.

TU Delft Solar Boat Team Delft, The Netherlands
Software Engineer September 2016 – August 2017
Designed and built a solar energy powered hydrofoil boat to compete in the Monaco Solar Boat challenge. I was responsible for the dashboard that starts up and controls the boat. During the races I monitored system status as part of our strategy team.

Awards

Best Cybersecurity Master Thesis Award in the Netherlands 2020

For my master thesis titled *'Adversarially Robust Decision Trees Against User-Specified Threat Models '*, supervised by Dr. Sicco Verwer.

Talks and tutorials

Robust Decision Trees Against Adversarial Examples October 2021
Seminar at University of Antwerp, invited by Guillermo Perez.

Skills

Programming Languages
Proficient in: Python, Java, JavaScript.
Familiar with: C/C++, Scala.

Tools and libraries
Gurobi, JAX, Scikit-learn, Git

Languages
Dutch (native), English (fluent)

Other interests

University Capture The Flag Hacking Team
I organize TU Delft's CTF team. Every year we organize a hacking competition for students and participate in international competitions ourselves to educate students about topics in cyber security. Currently, we are among the highest-rated Dutch teams on CTFtime.

Rowing and Sports
I like to do strength training, bouldering and rowing at Delft's student associations. Together with my rowing team we rowed a 100km marathon and collected donations for the Kika foundation.