Murat Bilgehan Ertan

me@mbertan.com LinkedIn Github ORCID mbertan.com

Education

Centrum Wiskunde & Informatica (CWI) - Vrije Universiteit Amsterdam **May 2025 – Apr 2029**
PhD Student in Security & Machine Learning *Amsterdam, Netherlands*

- PhD student under Prof. Marten van Dijk on privacy-preserving machine learning and the cryptographic foundations of trustworthy AI. Designing and evaluating cryptographic schemes for privacy-preserving generative models and studying refined Differential Privacy frameworks (e.g., f-DP) to balance privacy, generalization, and performance. Building and benchmarking privacy-preserving pipelines in PyTorch across deep learning and computer vision tasks.

Vrije Universiteit Amsterdam **Sep 2023 - Mar 2025**
MSc in Computer Security - Cum laude distinction *Amsterdam, Netherlands. cGPA: 9.1/10.0*

- Completed the two-year master's program in **1.5 years**, finishing six months ahead of schedule with a perfect thesis grade (10/10) and with a cumulative GPA of 9.1/10.0
- **Master's Thesis:** *ROAR: Robust Object Removal and Re-annotation*: proposed a scalable framework for privacy-preserving dataset obfuscation that removes sensitive objects using instance segmentation and generative inpainting, achieving strong privacy guarantees with minimal loss in detection and reconstruction performance. Supervised by Prof. Marten van Dijk.
- **Teaching Assistant (Nov 2023 – Jan 2024):** Assisted in the Secure Programming course, guiding weekly labs and discussions for a C++-based secure chat application project focused on applied cryptography and secure coding practices.
- **Key Courses:** Software Security (8.5/10), Network Security (8.5/10), Security and Machine Learning (10/10), Binary and Malware Analysis (8/10), Hardware Security (10/10), Advanced Operating Systems (8/10).

Sabancı University **Sep 2019 – June 2023**
BSc in Computer Science and Engineering *Istanbul, Turkey. cGPA: 3.59/4.00*

- **Key Courses:** Computer and Network Security, Artificial Intelligence, Machine Learning, Cybersecurity Practices and Applications
- **Honors:** Dean's List - High Honor (5 Semesters), Honor (1 Semester).
- Co-founded and co-led SUCyber, the university's cybersecurity student association, for three years. Designed and delivered an 8-week workshop series each semester covering Linux, network security, web exploitation, reverse engineering, and forensics.
- Contributed to community engagement through the Civil Involvement Project (CIP), volunteering in nursing homes and mentoring first-year students. Concurrently served as a board member of the Mimar ve Mühendisler Grubu (MMG) NGO, supporting educational outreach and student–industry collaboration for Architects and Engineers.

Work Experience

PRODAFT **Aug 2022 – May 2025**
Security Researcher & Developer *Netherlands, EC3 partner of EUROPOL*

- Worked on developing production-grade frameworks and pipelines both AI-driven and traditional for automated threat intelligence and security analysis. Utilized mostly C++ and Python to build scalable systems, integrating machine learning and LLM-based components to enhance detection, reasoning, and analyst support. One of the works led to the project *"Unveiling Cyber Threat Actors: A Hybrid Deep Learning Approach for Behavior-based Attribution."*, which resulted in a peer-reviewed publication in *ACM Digital Threats: Research and Practice (DTRAP)* 2024. [Paper Link].

KocLab **Mar 2022 – Feb 2023**
Research Assistant *Istanbul, Turkey*

- Worked under Prof. Çetin Kaya Koç on projects involving Reinforcement Learning and Cyber-Physical Security. Focused on applying reinforcement learning to improve the safety and navigation of autonomous drones, responsible for designing and implementing experimental setups using PEDRA.

Turkcell **Jun 2021 – Aug 2021**
Security Management & Architecture Intern *Istanbul, Turkey*

- Researched HTTP Secure Headers, Password Policies, Session Management, and JWT Token Security under the supervision of Necati Ersen Siseci.

Publications

M. B. Ertan, Zhu, X., Nguyen, P. H., van Dijk, M. and Devadas, S. "PACZero: PAC-Private Fine-Tuning of Language Models via Sign Quantization" *Under submission; 2026.* [arXiv preprint].

Marten van Dijk and **M. B. Ertan**. "Trade-off Functions for DP-SGD with Subsampling based on Random Shuffling: Tight Upper and Lower Bounds" *Under submission; 2026.* [arXiv preprint].

M. B. Ertan, and Marten van Dijk "Fundamental Limitations of Favorable Privacy–Utility Guarantees for DP-SGD" *Accepted ACM Conference on Computer and Communications Security (CCS)*, 2026. [arXiv preprint].

M. B. Ertan, Böge, E., Chen, M., Mahmood, K. and van Dijk, M. "On the Evidentiary Limits of Membership Inference for Copyright Auditing" *Under submission; 2026.* [arXiv preprint].

M. Damie, **M. B. Ertan**, D. Essoussi, A. Makhanu, G. Peter, R. Wensveen. "TOSSS: A CVE-based Software Security Benchmark for Large Language Models." *Under submission; 2026.* [arXiv preprint].

E. Böge, Y. Günindi, **M. B. Ertan**, E. Aptoula, N. Alp, H. Özkan. "A Biologically Inspired Filter Significance Assessment Method for Model Explanation." *The 3rd World Conference on eXplainable Artificial Intelligence (xAI-2025)*, Istanbul, Turkey, July 9–11, 2025. *Communications in Computer and Information Science (CCIS)*, Springer Nature, November 2025. [Springer Link]. Presented at the conference; slides available at [Sabancı University Research Repository].

M. B. Ertan, Sahu, R., Nguyen, P.H., Mahmood, K. and van Dijk, M. "Beyond Anonymization: Object Scrubbing for Privacy-Preserving 2D and 3D Vision." *Master's Thesis, Vrije Universiteit Amsterdam*, March 2025. [arXiv preprint]. Awarded final grade: 10/10.

M. B. Ertan, E. Böge (equal contribution), H. Alptekin, O. Çetin. "Unveiling Cyber Threat Actors: A Hybrid Deep Learning Approach for Behavior-based Attribution." *ACM Digital Threats: Research and Practice (DTRAP)*, Accepted June 2024. [Link to paper].

Programs & Activities

Young Talents in Cybersecurity 2025 (FR–NL Bilateral Program) **Mar 2025 – Oct 2025**

- Selected as one of 12 young talents from France and the Netherlands for a bilateral program sponsored by the Institut Français and both embassies.
- Gave a talk at **Forum InCyber FIC (Lille)**, **ONE Conference (The Hague)**, and the **MIT CAMS Research Community Discussion Group (Remote)**, presenting on LLM poisoning and secure code generation.
- Co-developed **TOSSS**, a benchmark for analyzing LLM poisoning in secure code generation, awarded first place in the 2025 challenge.

Technical Skills

Programming Languages: C, C++, Python, Node.JS, Golang, Assembly.
Tools: PyTorch & Opacus, Jax & Jax Privacy, Hugging Face (Transformers, Datasets), Ghidra, TensorFlow, Slurm (HPC).
Interests: Deep Learning, Computer Vision, Software Development, Reverse Engineering, Cryptography, Software Security, Differential Privacy.
Languages: Turkish (Native), English (Fluent), Dutch (A2)

Certificates

Participation in FR/NL Young Talents in Cybersecurity – Selected as 1 of 12 talents from France and the Netherlands, awarded by embassies from both countries.
VU-NT2 Cursus Alledaags Nederlands 1.1 (A0 → A1) – Successfully completed the course and passed the A1-level Dutch exam.
Certified Threat Intelligence Analyst – EC-Council awarded me the Certified Threat Intelligence Analyst certificate.
GitLab Certified Associate – Awarded by completing the GitLab associate course and passing the exam.
London College of Music Examinations Pianoforte – Grade 3 – Playing piano for nine years and achieved a Pianoforte certificate.