DOGUHAN YEKE

Website://doguhanyeke
Github://doguhanyeke
Linkedin://DoguhanYeke
305 N. University Street West Lafayette, IN 47907, USA ⋄ dyeke@purdue.edu ⋄ +1 (765) 701-9263

SUMMARY

I am a 5th-year (final-year) Ph.D. candidate in Computer Science at Purdue University, where I work as a systems security researcher in the PurSec Lab and CERIAS. My research primarily focuses on the security of **cyber-physical systems**, including autonomous systems, such as UAVs and mobile robots; **mobile security and privacy**, including smartphones and smartwatches; **deep learning applications** in security; and exploring attacks and defenses against **LLM agents**. Through system design, formal verification, static & dynamic analysis, and human-centered studies, my research explores safety- and security-critical vulnerabilities and proposes defenses to mitigate them.

EDUCATION

Purdue University *August 2021 - Ongoing*
Ph.D, Computer Science
Advisors: Prof. Z. Berkay Celik and Prof. Antonio Bianchi

Middle East Technical University (METU) *June 2017 - July, 2020*
M.Sc, Computer Engineering
*Graduated with the top grade, **Ranked 1st***
Thesis: Improving Document Ranking with Query Expansion based on BERT Word Embeddings
Advisor: Prof.Dr. Nihan Kesim Cicekli

Middle East Technical University (METU) *September 2013 - June 2017*
B.Sc, Computer Engineering, *Graduated with Honors*
Advisor: Prof. Yusuf Sahillioglu

PEER-REVIEWED PUBLICATIONS

C5 *CoRoB: A Systematic Framework for Multi-Robot Collision Avoidance Algorithms Under Sensor Attacks (in submission)*

C4 *ToT-Nav: Uncertainty-aware, Context-driven Robot Navigation with a Tree of Thoughts (in submission)*

C3 *From Read to Render: Display-Only Functionality for Permission-protected Data on Android (ongoing work)*

C2 **Doguhan Yeke**, Kartik A. Pant, Muslum Ozgur Ozmen, Hyungsub Kim, James M. Goppert, Inseok Hwang, Antonio Bianchi, Z.Berkay Celik
Automated Discovery of Semantic Attacks in Multi-Robot Navigation Systems
[Paper] , [Code]
The 34th USENIX Security Symposium (Security'25), 2025.

C1 **Doguhan Yeke**, Muhammad Ibrahim, Guliz Seray Tuncay, Habiba Farrukh, Abdullah Imran, Antonio Bianchi, and Z. Berkay Celik
Wear's my Data? Understanding the Cross-Device Runtime Permission Model in Wearables
[Paper], [Code], [Slides], [News]
Proceedings of the IEEE Security and Privacy (S&P), 2024.

TALKS

Sensor Attacks and Defenses in Interconnected Cyber-Physical Systems, Lightning Talk, Midwest Security Workshop, Indiana University Bloomington, September 2025.

Swarm Robots, Guest Lecturer in CS 36100: Great Issues in CS, Purdue University, February 2025.

Wear OS project, Android Security and Privacy Research (ASPIRE), Google (remote), October 2022

BUGS DISCOVERED

Location Privacy Leaks, awarded 500$ bug bounty by Google, 2023.

AWARDS AND HONORS

2025: Served at the Student Advisory Council of **NSF AI** Institute for Agent-based Cyber Threat Intelligence and Operation (ACTION), 2025-2026.

2024: Thrilled to be named as a **Windracers Fellow**.

2023: Served at the **NSF ACTION GATE**, Institute for Agent-based Cyber Threat Intelligence and Operation, 2023.

2023: Student contributor of **Google ASPIRE Award**.

2022: Student contributor of **Google ASPIRE Award**.

2021: **Interpersonal Conversation Partner** at Purdue University.

2019: **Best Course Performance Award** at METU.

2019: **Highest Departmental cGPA** in all graduates of Master's Degree at METU.

2013-2017: **High Honor Student** in multiple semesters of Bachelor's Degree at METU.

2011-2012: Ranked 5th in Turkey in **Mathematics Olympiads** in High School conducted by the Scientific and Technological Research Council of Turkey (TUBITAK), sponsored by OYAK.

ACADEMIC AND RESEARCH EXPERIENCE

Lead Graduate Student *May 2025 - Ongoing*
Prof. Celik's Research Group, Purdue University

- Mentoring students and holding group meetings

Department of Computer Science at Purdue University *August 2021 - Ongoing*
Research Assistant

- Working on cyber-physical systems and mobile systems.
- TA in Data Structures (CS 251) and Software Engineering (CS 307).

Department of Computer Engineering at METU *August 2018 - July 2021*
Research and Teaching Assistant

- CEng492: Computer Engineering Design, CEng489: Introduction to Computer Security, CEng350: Software Engineering, CEng331: Computer Organization

eNTERFACE at University of Mons, Belgium *June 2015 - August 2015*
Undergraduate Research Assistant

- Implemented Python modules for the classification of very large number of objects and used the Neo4j Graph database to visualize the classification results.

TSK Modsimmer *August 2015 - September 2015*

Summer Internship

- Wrote a simulation of a fireforest using C++ with concurrency and implemented an interface with QT.
- Given a point of fire, the program estimates where the fire will spread using different parameters like wind speed and tree population.

Department of Computer Engineering at METU *September 2015 - January 2015*

Undergraduate Teaching Assistant

- CEng230: Introduction to C Programming

INDUSTRIAL EXPERIENCE

Comodo, Turkey *June 2017 - August 2018*

Software Developer

- Worked as a Backend Developer: used different tech stacks like Flask, Express, Javascript, Relational Databases, REST APIs, Redis, AWS and testing, etc.
- Worked as a Security Researcher: implemented Deep Learning models for detecting malware and integrating third-party libraries into our system.
- Worked with static and dynamic analysis tools such as Cuckoo to detect the malware.

SAP Development Center *June 2016 - September 2016*

Student(Intern) Software Developer

- Worked in the Security team as a Golang developer in an agile team during my internship.

SERVICES

- External reviewer at IEEE S&P 2026, 2024, 2023,
- External reviewer at USENIX Security 2024,
- External reviewer at NDSS 2026, 2023,
- External reviewer at ACM WiSec 2024.

TEACHING

Teaching Assistant, Purdue University *August 2021 - August 2026*

- CS 307: Software Engineering I (Undergraduate) [Fall 2023, Fall 2022]
- CS 251: Data Structures (Undergraduate) [Spring 2022, Fall 2021]

Teaching Assistant, METU *August 2019 - August 2021*

- CEng492: Computer Engineering Design
- CEng489: Introduction to Computer Security
- CEng350: Software Engineering
- CEng331: Computer Organization

MENTEES

- Marcelo Moreno Wong, Senior, Purdue University
- Apoorva Vashisth, PhD, Purdue University
- Kai Cheng, PhD, Purdue University

- Qingyi Chen, PhD, Purdue University
- Baran Yanci, Senior, METU
- Cem Meric Sefikogullari, Senior, METU
- Arda Numanoglu, Senior, METU
- Yahya Sungur, Senior, METU

PROJECTS

NSF AI ACTION GATE *Jan 2024 - Ongoing*
NSF AI Institute for Agent-based Cyber Threat Intelligence and Operation (ACTION)

- Collaborated with UCSB and GaTech to design and develop GATE infrastructure.
- Deployed digital twins of water plant and chemical plant, and demonstrated an end-to-end attack.
- Deployed attack and defense agents.

Industrial Control System Modeling with SCEPTRE Framework *May 2022 - October 2022*
Sandia National Laboratories

- Collaborated with Sandia Labs while studying at Purdue University in the summer of 2022.
- Deployed Cyber Emulation, Modeling, and Analysis Tools on the SOL4CE.

TECHNICAL STRENGTHS

Tools: FlowDroid, Tensorflow, VectorDB, RAG, PX4, Ardupilot, Gazebo, Formal Methods, Cuckoo Sandboxing, Keras, PyTorch, AWS, RabbitMQ, React, Redux, Node.js, Express, MongoDB, Typescript, Mongoose, AWS Services, In-memory database.
Languages: Python, C++, C, JavaScript, Java, Scala, R, Assembly, Haskell, Verilog, Rust.
Toefl Score: 100 Reading: 26, Listening: 26, Speaking: 25, Writing: 23
GRE Score: Quantitative: 167, Verbal: 141, Analytical Writing: 3,5

COURSES TAKEN

Undergraduate Courses: Object Oriented Programming, Cloud Computing, Machine Learning
Graduate Courses: Information Security, IoT Security, Distributed Systems, Computer Networks, Algorithms, Big Data Analytics, Advanced Deep Learning, Statistical Data Analysis, Information Retrieval, Computational Geometry, Algorithmic Trading