Onur Duman · Postdoctoral Research Fellow · Oslo, Norway · Onur.Duman@kristiania.no · onurduman.ca

Onur Duman | Resume

- **Status:** Postdoctoral Research Fellow at Kristiania University College
- **Fields:** Network Security Research, Threat Modeling, Security Metrics, Security Evaluation, Cryptography, Cryptanalysis, Software Engineering
- **Tech:** Linux, Kali Linux, Parrot OS, Bash, Python, Java, C, C++, MATLAB, HTML, CSS, Git, MongoDB, PHP, SQL, MySQL, pandas, NumPy
- **Loves:** Movies, Reading, Stack Overflow, TryHackMe, HackTheBox, Coding, Learning, Traveling, Fitness, History
- **Languages:** English (Advanced), Turkish (Native), French (Fluent)

Professional Experience

2023/09 - Present — **Postdoctoral Research Fellow** — Kristiania University College

- Working on developing web application security test as part of the project EAST.
- This work is an ongoing open-source project, called Evomaster .
- Supervisor: Prof. Andrea Arcuri
- **Skills:** Automated software testing, Spring Boot, Java, Kotlin, REST, Fuzzing

2016/09 - 2023/09 — **Smart Grid Security Research Assistant** — Concordia University

- Develop a threat modeling framework that measures the security posture based on information from different sources (Ongoing)
- Implement a hardening framework to improve the security posture of IEC 61850 substations concerning different security metrics (Ongoing)
- Define a novel security metric, namely Factor of Security (FoS), for measuring how well redundancy is designed from a security perspective, and validate it with simulations
- Design and validate a novel security metric, namely kSupply, to measure the security posture of IEC 61850 substations against supply chain hijacking attacks
- **Skills:** VirtualBox, VMware, NumPy, MongoDB, pandas, Data Analysis, Threat Modeling, LaTeX, Security Metrics, MySQL, OOP, Research, Linux, Kali Linux, MATLAB, Python

2015/01 - 2023/09 — **Teaching Assistant** — Concordia University

- Grader and lab demonstrator for INSE 6120, INSE 6130, and INSE 6140
- Teaching assistant for a Java programming course
- Lab mentor and teaching assistant for a digital design course
- **Skills:** Network Security, Information Security, Java, Kali Linux, VMware, VirtualBox

2015/01 - 2016/06 — **Cryptography Research Assistant** — Concordia University

- Apply differential fault analysis to the standard cipher, Kuznyechik, and demonstrate that its secret key can be recovered using an average of four faults
- Demonstrate that the cipher Kalyna can be broken using an average of three faults
- Validate that the standard hash function Kupyna can be broken using fault analysis
- **Skills:** VirtualBox, VMware, LaTeX, Information Security, Cybersecurity, Research, Linux, C, C++, Python, Cryptography, AES, Fault Analysis

2013/11 - 2015/01 — **Freelance Software Developer** — Herakles Consulting

- Design, implement, and maintain websites for several organizations
- Work on a contract that involves improving features of a web application
- **Skills:** HTML, CSS, PHP, MySQL, Python, Git

2013/03 - 2013/09 **Software Quality Assurance Test Specialist** — Accedian Networks

- Automate many test cases which reduce the time needed to test and verify devices
- Save money for the company by identifying some important bugs before devices, which are worth hundreds of thousands, are shipped
- Keep track of test results to identify bugs early during development
- **Skills:** Python, Linux, Wireshark, Hudson Framework, C

2011/04 - 2013/02 **Software Engineer** — Nuance Communications Inc.

- Develop Nuance Development Integration Platform (NDIP) from scratch for automating the process of deployment and running tests after modifications in the source code, which saves the time required for verification before release
- Develop unit tests for different components of the project Nuance Voice Recognition (NVC) which ended up as releasing the product with fewer bugs
- Implementation of the log analyzer component of NVC, which extracts important information from system logs obtained from different components
- **Skills:** Java, Python, Linux, VMware

Education

2016/09 - 2023/12 **Ph.D. in Information & Systems Engineering** — Concordia University

- Supervisors: Prof. Lingyu Wang and Prof. Mourad Debbabi
- Thesis Topic: Measuring and improving the security posture of IEC 61850 substations with respect to different types of cyber attacks
- The purpose of my Ph.D. is to design security metrics for risk assessment, which helps organizations to improve their security posture, and prevent cyber-physical attacks
- GPA: 4.3/4.3

2015/01 - 2016/06 **Master of Applied Science in Information Systems Security** — Concordia University

- Supervisor: Prof. Amr Youssef
- Thesis Title: Application of Fault Analysis to Some Cryptographic Standards
- The purpose of my Master's is to demonstrate how some cryptographic standards can be broken using fault analysis
- GPA: 4.3/4.3

2008/09 - 2011/01 **Master of Science (Non-Thesis)** — McGill University

- Project Title: Addition of Account Creation and Login functionalities to the Multiplayer Game, Mammoth
- Integrate a newly designed protocol for remote procedure calls to add login, and chatting functionalities to Mammoth, which is a massively multiplayer online game

2004/09 - 2011/01 **Bachelor of Engineering, Department of Computer Engineering** — Bilkent University

- Senior Project Title: Mobile Search Engine for Restaurants and Activities in the City
- High honor student for all terms
- Received success scholarship for three years which includes a full tuition fee waiver
- GPA: 3.88/4.00 (4th best GPA)

Publications

Journal

1. Riham AlTawy, **Duman, Onur**, and Amr M Youssef. Fault Analysis of Kuznyechik. *Mathematical Aspects of Cryptography*, 7(2):21–34, 2016

2. **Duman, Onur** and Amr M Youssef. Fault Analysis on Kalyna. *Information Security Journal: A Global Perspective*, 26(5):249–265, 2017

3. **Duman, Onur**, Mengyuan Zhang, Lingyu Wang, Mourad Debbabi, Ribal Atallah, and Bernard Lebel. Factor of Security (FoS): Quantifying the Security Effectiveness of Redundant Smart Grid Subsystems. *IEEE Transactions on Dependable and Secure Computing*, 2020

Conference

1. **Duman, Onur**, Mengyuan Zhang, Lingyu Wang, and Mourad Debbabi. Measuring the Security Posture of IEC 61850 Substations with Redundancy Against Zero Day Attacks. In *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pages 108–114. IEEE, 2017

2. **Duman, Onur** and Amr Youssef. Fault Analysis of the New Ukrainian Hash Function Standard: Kupyna. In *International Symposium on Foundations and Practice of Security*, pages 225–240. Springer, 2018

3. **Duman, Onur**, Mohsen Ghafouri, Marthe Kassouf, Ribal Atallah, Lingyu Wang, and Mourad Debbabi. Modeling Supply Chain Attacks in IEC 61850 Substations. In *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pages 1–6. IEEE, 2019

4. **Duman, Onur**, Lingyu Wang, Minh Au, Marthe Kassouf, and Mourad Debbabi. Hardening Substations against Supply Chain Attacks Under Operational Constraints. In *2022 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, pages 1–5. IEEE, 2022

5. Abolfazl Rahiminejad, **Onur Duman**, Mohsen Ghafouri, Ribal Atallah, Arash Mohammadi, and Mourad Debbabi. A Resilience Quantitative Framework for Wide Area Damping Control Against Cyberattacks. In *2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*. IEEE, 2023

Awards and Distinctions

1. Ranked 1240th among 1,728,076 students in the University Entrance Exam in Turkey (OSS) in 2004
2. Bilkent University Success Scholarship for 2005 - 2006 (8370 USD)
3. Bilkent University Success Scholarship for 2006 - 2007 (8370 USD)
4. Bilkent University Success Scholarship for 2007 - 2008 (8370 USD)
5. McGill University Graduate Fellowship Award (1,500 CAD)
6. Concordia Conference and Exposition Award for attending CTCrypt 2015 (1,000 CAD)
7. Concordia Conference and Exposition Award for attending IEEE SmartGridComm 2017 (1,000 CAD)
8. Concordia Conference and Exposition Award for attending IEEE SmartGridComm 2019 (1,000 CAD)
9. Concordia Conference and Exposition Award for attending FPS 2018 (1,000 CAD)
10. Concordia Merit Scholarship for the 2016 academic year (10,000 CAD)
11. Concordia Merit Scholarship for the 2017 academic year (10,000 CAD)
12. Concordia Graduate Fellowship D ENCS for Ph.D. (32,400 CAD)
13. Completed online training titled “Computer Security and Systems Management” in Coursera
14. Completed training titled “Comprehensive Project Management” at McGill University
15. Completed training titled “Effective Public Speaking” at McGill University
16. Finalist of the 2020 Turkish intelligence competition organized by the Turkish Intelligence Foundation
17. Ranked in the top 5% among users of tryhackme.com (https://tryhackme.com/p/herakles)
18. Obtained a 5-star gold badge for problem-solving in Hackerrank (https://www.hackerrank.com/dumanonur)

Professional Activities

1. Paper reviewer for IEEE Transactions on Industrial Informatics, IEEE Transactions on Dependable and Secure Computing, ACM Transactions on Internet Technology, IEEE Communication Letters, IEEE Transactions on Reliability, Computers & Security, International Journal of Critical Infrastructure Protection, ESORICS, IFIP International Conference on Security and Privacy, Annual Symposium on Information Assurance (ASIA), ICC

2. Program commitee member of ACM CCS 2023 Poster Session

Volunteering

1. Student mentor for final-year undergraduate students at Bilkent University, as part of “Bilkent University Mentorship Program”
2. Worked as a photographer at the international conference, Foundations and Practice of Security (FPS) 2018
3. Helped with event organizations in Concordia Multi-faith & Spirituality Center