Muslum Ozgur Ozmen

✉ mozmen@purdue.edu ☎ +1 (541) 908-5783
https://ozgurozmen.github.io/ · Google Scholar · https://github.com/ozgurozmen

Education

Jan 2020 — May 2024	**Ph.D. in Computer Science** 4.00/4.00 Advisor: Prof. Z. Berkay Celik Committee Members: Prof. Dongyan Xu, Prof. Xiangyu Zhang, Prof. Antonio Bianchi Purdue University — West Lafayette, IN, USA
Sept 2016 — June 2018	**MS in Computer Science** 3.96/4.00 Advisor: Prof. Attila Altay Yavuz Oregon State University — Corvallis, OR, USA
Sept 2012 — June 2016	**BS in Electrical and Electronics Engineering** 3.49/4.00 Bilkent University — Ankara, Turkey

Research Interests

My research interests broadly lie in the area of **system security**. Through **system design**, **formal verification**, **machine learning**, and **applied cryptography**, my research seeks to improve the security and privacy guarantees in emerging computing platforms and their interactions with physical spaces. My research approach is best illustrated by my work in IoT safety and security.

Research and Professional Experience

Lead Graduate Student - Prof. Celik's Research Group, Purdue University 2022 - Present

- Hold regular meetings with 3 undergraduate and 5 graduate students to guide their research
- Organize writing workshops to show group members how to structure and write papers

Cyber-Physical Systems Research Intern - Toyota Research Institute North America 2023
Supervisors: Dr. Georgios Fainekos and Dr. Bardh Hoxha

- Conducted research on the safety and security of mobile robots
- Developed an optimization-guided falsification framework for control barrier function-based controllers

Publications

Peer-reviewed conference publications:

C24 Hyungsub Kim, Rwitam Bandyopadhyay, **Muslum Ozgur Ozmen**, Z. Berkay Celik, Antonio Bianchi, Yongdae Kim and Dongyan Xu. *A Systematic Study of Physical Sensor Attack Hardness.* IEEE S&P 2024. (Acceptance Rate: TBD)

C23 Arjun Arunasalam, Andrew Chu, **Muslum Ozgur Ozmen**, Habiba Farrukh, and Z. Berkay Celik. *The Dark Side of E-Commerce: Dropshipping Abuse as a Business Model.* Network and Distributed System Security Symposium (NDSS) 2024. (Acceptance Rate: 19%)

C22 **Muslum Ozgur Ozmen**, Ruoyu Song, Habiba Farrukh and Z. Berkay Celik. *Evasion Attacks and Defenses on Smart Home Physical Event Verification.* Network and Distributed System Security Symposium (NDSS) 2023. (Acceptance Rate: 16.2%)

C21 Habiba Farrukh*, **Muslum Ozgur Ozmen***, Kerem Ors and Z. Berkay Celik. *One Key to Rule Them All: Secure Group Pairing for Heterogeneous IoT Devices.* IEEE S&P 2023. – equally contributed. (Acceptance Rate: 17%)

C20 **Muslum Ozgur Ozmen***, Habiba Farrukh*, Hyungsub Kim, Antonio Bianchi and Z. Berkay Celik. *Rethinking Secure Pairing in Drone Swarms.* VehicleSec 2023. – equally contributed.

C19 Ruoyu Song, **Muslum Ozgur Ozmen**, Hyungsub Kim, Raymond Muller, Z. Berkay Celik, and Antonio Bianchi. *Discovering Adversarial Driving Maneuvers against Autonomous Vehicles.* Usenix Security 2023. (Acceptance Rate: 29%)

C18 Hyungsub Kim, **Muslum Ozgur Ozmen**, Z. Berkay Celik, Antonio Bianchi and Dongyan Xu. *PatchVerif: Discovering Faulty Patches in Robotic Vehicles.* Usenix Security 2023. (Acceptance Rate: 29%)

C17 Khaled Serag, Rohit Bhatia, Akram Faqih, **Muslum Ozgur Ozmen**, Vireshwar Kumar, Z. Berkay Celik, Dongyan Xu. *ZBCAN: A Zero-Byte CAN Defense System.* Usenix Security 2023.(Acceptance Rate: 29%)

C16 **Muslum Ozgur Ozmen**, Xuansong Li, Andrew Chu, Z. Berkay Celik, Bardh Hoxha and Xiangyu Zhang. *Discovering IoT Physical Channel Vulnerabilities.* ACM Conference on Computer and Communications Security (ACM CCS) 2022. (Acceptance Rate: 22%)

C15 Hyungsub Kim, **Muslum Ozgur Ozmen**, Z. Berkay Celik, Antonio Bianchi and Dongyan Xu. *PGPATCH: Policy-Guided Logic Bug Patching for Robotic Vehicles.* IEEE S&P 2022. (Acceptance Rate: 14.5%)

C14 Andrew Chu, Arjun Arunasalam **Muslum Ozgur Ozmen** and Z. Berkay Celik. *Behind the Tube: Exploitative Monetization of Content on YouTube.* Usenix Security 2022. (Acceptance Rate: 17.2%)

C13 Hyungsub Kim, **Muslum Ozgur Ozmen**, Antonio Bianchi, Z. Berkay Celik and Dongyan Xu. *PGFUZZ: Policy-Guided Fuzzing for Robotic Vehicles.* Network and Distributed System Security Symposium (NDSS) 2021. (Acceptance Rate: 15.2%)

C12 Furkan Goksel*, **Muslum Ozgur Ozmen***, Michael Reeves, Basavesh Shivakumar and Z. Berkay Celik. *On the Safety Implications of Misordered Events and Commands in IoT Systems.* IEEE Workshop on the Internet of Safe Things (SafeThings) 2021. – equally contributed.

C11 Rouzbeh Behnia, Attila Yavuz, **Muslum Ozgur Ozmen** and Tsz Hon Yuen. *Compatible Certificateless and Identity-Based Cryptosystems for Heterogeneous IoT.* International Conference on Information Security (ISC) 2020.

C10 Efe U. A. Seyitoglu, Attila Yavuz and **Muslum Ozgur Ozmen**. *Compact and Resilient Cryptographic Tools for Digital Forensics.* IEEE Conference on Communications and Network Security (IEEE CNS) 2020. **(Best Paper Award Finalist)**

C9 **Muslum Ozgur Ozmen**, Attila Yavuz and Rouzbeh Behnia. *Energy-Aware Digital Signatures for Embedded Medical Devices.* IEEE Conference on Communications and Network Security (IEEE CNS) 2019.

C8 Rouzbeh Behnia, **Muslum Ozgur Ozmen** and Attila Yavuz. *ARIS: Authentication for Real-Time IoT Systems.* International Conference on Communications (IEEE ICC) 2019.

C7 **Muslum Ozgur Ozmen**, Rouzbeh Behnia and Attila Yavuz. *Fast Authentication from Aggregate Signatures with Improved Security.* Financial Cryptography and Data Security (FC) 2019. (Acceptance Rate: 21.9%)

C6 Rouzbeh Behnia, **Muslum Ozgur Ozmen**, Attila Yavuz and Mike Rosulek. *TACHYON: Fast Signatures from Compact Knapsack.* ACM Conference on Computer and Communications Security (ACM CCS) 2018. (Acceptance Rate: 16.6%)

C5 **Muslum Ozgur Ozmen** and Attila Yavuz. *Dronecrypt-An Ultra-Low Energy Cryptographic Framework for Small Aerial Drones.* IEEE MILCOM 2018.

C4 **Muslum Ozgur Ozmen**, Rouzbeh Behnia and Attila Yavuz. *Compact Energy and Delay-Aware Authentication.* IEEE Conference on Communications and Network Security (IEEE CNS) 2018.

C3 **Muslum Ozgur Ozmen**, Thang Hoang and Attila Yavuz. *Forward-Private Dynamic Searchable Symmetric Encryption with Efficient Search.* International Conference on Communications (IEEE ICC) 2018.

C2 **Muslum Ozgur Ozmen** and Attila Yavuz. *Low-Cost Standard Public Key Cryptography Services for Wireless IoT Systems.* Workshop on Internet of Things Security and Privacy (IoT S&P) 2017 (Affiliated with ACM CCS).

C1 Rouzbeh Behnia, Attila Yavuz and **Muslum Ozgur Ozmen**. *High-Speed High-Security Public Key Encryption with Keyword Search.* IFIP Annual Conference on Data and Applications Security and Privacy (DBSec) 2017.

Peer-reviewed journal publications:

J4 **Muslum Ozgur Ozmen**, Habiba Farrukh and Z. Berkay Celik. *A Systematic Study of Physical Sensor Attack Hardness.* Conditionally Accepted to Proceedings on Privacy Enhancing Technologies (PoPETs) 2024. (Acceptance Rate: 19.5%)

J3 Attila Yavuz and **Muslum Ozgur Ozmen**. *Ultra Lightweight Multiple-time Digital Signature for the Internet of Things Devices.* IEEE Transactions on Services Computing (IEEE TSC), 2019.

J2 Thang Hoang, **Muslum Ozgur Ozmen**, Yeongjin Jang and Attila Yavuz. *Hardware-Supported ORAM in Effect: Practical Oblivious Search and Update on Very Large Dataset.* Proceedings on Privacy Enhancing Technologies (PoPETs), 2019. (Acceptance Rate: 22%)

J1 Rouzbeh Behnia, **Muslum Ozgur Ozmen** and Attila Yavuz. *Lattice-Based Public Key Encryption with Keyword Search from Experimental Perspectives.* IEEE Transactions on Dependable and Secure Computing (IEEE TDSC), 2018.

Patents

P3 Rouzbeh Behnia, **Muslum Ozgur Ozmen** and Attila Yavuz. *Efficient Identity-Based and Certificateless Cryptosystems*, US Patent 10,673,625

P2 Attila Yavuz, **Muslum Ozgur Ozmen** and Rouzbeh Behnia. *Energy-aware Digital Signatures*, US Patent 10,547,455

P1 Thang Hoang, **Muslum Ozgur Ozmen**, and Attila Yavuz *Forward-Private Dynamic Searchable Symmetric Encryption with Efficient Search*, US Patent 10,922,273

Teaching Experience

Guest Lecturer:

- CS426 - Computer Security, Purdue University — Spring 2023
- CS590 - IoT & CPS Security, Purdue University — Spring 2022

Teaching Assistant:

- CS496 - Mobile and Cloud Software Development, Oregon State University — Winter 2018
- CS261 - Data Structures, CS/ECE578 - Cyber-security, Oregon State University — Fall 2017
- CS492 - Mobile Software Development, Oregon State University — Winter 2017

Presentations

Invited Talks:

I2 *Compositional Safety and Security Reasoning in IoT Environments.* University of California Santa Cruz. Virtual, February 2023.

I1 *Lightweight, Delay-Aware and Scalable Cryptographic Services for Smart-Grid Systems.* Cyber Resilient Energy Delivery Consortium (CREDC) Pacific Northwest Industry Workshop. Richland, WA, USA, November 2017.

Conference and Workshop Talks:

T7 *Evasion Attacks on Smart Home Physical Event Verification and Defenses.* Network and Distributed System Security Symposium (NDSS). San Diego, CA, USA, March 2023.

T6 *Discovering IoT Physical Channel Vulnerabilities.* ACM Conference on Computer and Communications Security. Los Angeles, CA, USA, November 2022.

T5 *Energy-Aware Digital Signatures for Embedded Medical Devices.* IEEE Conference on Communications and Network Security. Washington, DC, USA, June 2019.

T4 *Fast Authentication from Aggregate Signatures with Improved Security.* Financial Cryptography and Data Security. St Kitts and Nevis, February 2019.

T3 *TACHYON: Fast Signatures from Compact Knapsack.* ACM Conference on Computer and Communications Security. Toronto, ON, Canada, October 2018.

T2 *Forward-Private Dynamic Searchable Symmetric Encryption with Efficient Search.* IEEE International Conference on Communications. Kansas City, MO, USA, May 2018.

T1 *Low-Cost Standard Public Key Cryptography Services for Wireless IoT Systems.* Workshop on Internet of Things Security and Privacy. Dallas, TX, USA, November 2017.

Student Research Mentoring

Ben Chen	MS Computer Science, Purdue University	2022 - Present
Andrew Chu	BS Computer Science, Purdue University → Ph.D. University of Chicago	2020-2021
Ruoyu Song	BS Computer Science, Purdue University → Ph.D. Purdue University	2020
Furkan Goksel	BS Computer Science, METU → Picus Security	Summer 2020
Kerem Ors	BS Computer Science, Sabanci Uni → Ph.D. Purdue University	Summer 2020

Services

Program Committee Member:

- ACM Conference on Data and Application Security and Privacy (CODASPY) 2024
- IEEE Secure Development Conference (SecDev) 2024
- Symposium on Vehicle Security and Privacy (VehicleSec) 2024
- IEEE International Conference on Smart Grid Communications (SmartGridComm) 2023
- Workshop on CPS&IoT Security and Privacy (CPSIoTSec) 2023
- IEEE/ACM Workshop on the Internet of Safe Things (SafeThings) 2023, 2024
- ICDM Machine Learning for Cybersecurity (MLC) 2023
- Workshop on Re-design Industrial Control Systems with Security (RICSS) 2023

Reviewer:

- IEEE Transactions on Dependable and Secure Computing (TDSC) - 2024
- ACM Transactions on Internet Technology (TOIT) - 2024
- ACM Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT/Ubicomp) - 2023
- IEEE Transactions on Information Forensics and Security - 2023
- ACM Transaction on Internet of Things - 2023
- IEEE Internet of Things Journal - 2022, 2024
- Journal of Complex & Intelligent Systems - Springer, 2021
- IEEE Transactions on Services Computing - 2020
- IEEE Access - 2019
- Journal of Ambient Intelligence and Humanized Computing - Springer, 2018

External Reviewer:

- IEEE Symposium on Security and Privacy (S&P) 2023, 2024
- Usenix Security 2022, 2023, 2024
- Network and Distributed System Security Symposium (NDSS) 2022, 2023, 2024
- ACM Conference on Computer and Communications Security (CCS) 2021
- Annual Computer Security Applications Conference (ACSAC) 2017, 2018, 2019, 2022
- International World Wide Web Conference (WWW) 2019

Awards and Honors

- Served at the Student Advisory Council of *NSF AI Institute for Agent-based Cyber Threat Intelligence and Operation (ACTION)*, 2023.
- Invited as a panelist to *NSA's Center of Academic Excellence in Cybersecurity Research Symposium 2023* to present my dissertation research on IoT/CPS security to practitioners and government agencies for real-world adoption.
- Recipient of NDSS 2023 Travel Grant ($1,550).
- IEEE CNS 2020 Best Paper Award Finalist
- Recipient of IEEE CNS 2019 Travel Grant ($1,250).
- Turkish Educational Foundation, Outstanding Success Scholarship (awarded to 50 students nationwide), September 2013 — June 2016.