ABDULLAH AL ARAFAT

aalaraf@ncsu.edu • https://abdullahaarafat.github.io/

RESEARCH INTERESTS

- Real-Time Computing and Scheduling Theory
- Robust Learning Theory
- Formal Methods and Control Theory
- Cyber-physical Systems

EDUCATION

Ph.D. in Computer Science May 2025 (Expected)
North Carolina State University, Raleigh, NC
Dissertation Title (tentative): Towards Resilient and Secure Real-Time Intelligent Systems
Advisor: Dr. Zhishan Guo

M.Sc. in Computer Engineering May 2020
University of Central Florida, Orlando, FL

B.Sc. in Electrical & Electronic Engineering March 2016
Bangladesh University of Engineering and Technology, Dhaka

RESEARCH EXPERIENCE

Graduate Research Assistant
North Carolina State University, Raleigh, NC Fall 2022 - Present
University of Central Florida, Orlando, FL Fall 2019 - Summer 2022

TEACHING EXPERIENCE

Instructor
North Carolina State University, Raleigh, NC

- CSC 714: Real-time Computer Systems (co-teach with Dr. Zhishan Guo) Spring'24
  Teaching Evaluation (students' rating): 4.80 out of 5.00

Graduate Teaching Assistant
North Carolina State University, Raleigh, NC

- CSC 495: Advanced Algorithms Spring'23, Fall'23
- CSC 520: Artificial Intelligence Fall'23
- CSC 591/714: Real-Time Computer Systems Spring'24

University of Central Florida, Orlando, FL

- EEL 4742C: Embedded System Spring'21, Summer'21, Spring'22, Summer'22
- EEL 3801C: Computer Organization Summer'21
- EEL 4768: Computer Architecture Summer'21
- EEE 4775: Real-Time Systems Fall'21
- EEE 4346: Hardware Security and Trusted Circuit Design Fall'21

- EGN 3211: Engineering Analysis and Design Spring'22
- EEL 4781: Computer Communication Networks Summer'22

PUBLICATIONS

Research Summary

I have published **12** top-tier journals and conference papers on topics related to secure and resilient real-time cyber-physical systems. I have a total of **8 papers published at the prestigious CSRankings** listed conferences. My DAC 2022 paper was recognized as a **Publicity Paper** at the conference. Following is the list of papers for each research topic:

Real-Time Scheduling	**RTAS2023, RTSS2023**
Robot Operating System (ROS 2)	**DAC2022, EMSOFT2024**
Robust Learning/AI Security	**VR2021, ICCV2023, ECCV2024, CCS2024**
End-to-end Verification/Formal Methods	**MEMOCODE2024**

Note: Authors with '*' contributed equally to the paper.

Conferences

8. **Abdullah Al Arafat***, Nazmul Karim*, Adnan Siraj Rakin, Zhishan Guo, Nazanin Rahnavard. '*Fisher Information Guided Purification against Backdoor Attacks*' in 31st ACM Conference on Computer and Communications Security **(CCS)**, 2024.

7. **Abdullah Al Arafat***, Nazmul Karim*, Umar Khalid, Zhishan Guo, Nazanin Rahnavard. '*Augmented Neural Fine-Tuning for Efficient Backdoor Purification*' in The European Conference on Computer Vision **(ECCV)**, 2024.

6. **Abdullah Al Arafat**, Kurt Wilson, Kecheng Yang, Zhishan Guo. '*Dynamic Priority Scheduling of Multi-Threaded ROS 2 Executor with Shared Resources*' in ACM SIGBED International Conference on Embedded Software **(EMSOFT)**, 2024.

5. Zhishan Guo*, Sudharsan Vaidhun*, **Abdullah Al Arafat***, Nan Guan, and Kecheng Yang. '*Stealing Static Slack via WCRT and Sporadic P-Servers in Deadline-Driven Scheduling*' 44th IEEE Real-Time Systems Symposium **(RTSS)**, 2023.

4. **Abdullah Al Arafat***, Sabbir Ahmed*, Mamshad Nayeem Rizve*, Rahim Hossain, Zhishan Guo, and Adnan Siraj Rakin. '*SSDA: Secure Source-Free Domain Adaptation*' in International Conference on Computer Vision **(ICCV)**, 2023.

3. **Abdullah Al Arafat**, Sudharsan Vaidhun, Liangkai Liu, Kechang Yang, and Zhishan Guo. '*Compositional Mixed-Criticality Systems with Multiple Executions and Resource-Budgets Model*' in 29th IEEE Real-Time and Embedded Technology and Applications Symposium **(RTAS)**, 2023.

2. **Abdullah Al Arafat**, Sudharsan Vaidhun, Kurt M. Wilson, Jinghao Sun, and Zhishan Guo. '*Response Time Analysis for Dynamic Priority Scheduling in ROS2*' in 59th IEEE/ACM Design Automation Conference **(DAC)**, 2022. (Publicity Paper Award) [News coverage]

1. **Abdullah Al Arafat**, Zhishan Guo, and Amro Awad. '*VR-Spy: A Side-Channel Attack on Virtual Key-Logging in VR Headsets*' in IEEE Conference on Virtual Reality and 3D User Interfaces **(IEEE VR)**, 2021.

Journals

2. **Abdullah Al Arafat**, Kurt Wilson, Kecheng Yang, Zhishan Guo. '*Dynamic Priority Scheduling of Multi-Threaded ROS 2 Executor with Shared Resources*' in IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems **(TCAD)**, 2024.

1. **Abdullah Al Arafat***, Jiang Bian*, Haoyi Xiong, Jing Li, Li Li, Hongyang Chen, Jun Wang, Dejing Dou, and Zhishan Guo. '*Machine Learning in Real-Time Internet of Things (IoT) Systems: A Survey*' in IEEE Internet of Things Journal **(IoT-J)**, 2022.

Workshops and Work-in-Progresses

5. Kurt Wilson, **Abdullah Al Arafat**, John Baugh, Ruozhou Yu, Zhishan Guo. '*SOTERIA: A Formal Verification Framework for Latency-Aware Safety-Critical Systems*' in submission.

4. **Abdullah Al Arafat**, Kurt Wilson, Sudharsan Vaidhun, Bryan C. Ward, Zhishan Guo. '*Memory-Corruption Resilient Real-Time Recovery Model and Analysis*' in submission.

3. Sabbir Ahmed, Mamshad Nayeem Rizve, Jacqueline Tiffany Liu, **Abdullah Al Arafat**, Rahim Hossain, Mohaiminul Al Nahian, Adnan Siraj Rakin. '*Unified Alignment Protocol for Generalized Semi-Supervised Federated Learning*' in submission.

2. Kurt Wilson, **Abdullah Al Arafat**, John Baugh, Ruozhou Yu, Zhishan Guo. '*Work-In-Progress: Physics-Aware Mixed-Criticality Systems Design via End-to-End Verification of CPS*' in 22nd International Symposium on Formal Methods and Models for System Design **(MEMOCODE)**, 2024.

1. **Abdullah Al Arafat**, Sudharsan Vaidhun, Bryan C. Ward, and Zhishan Guo. '*A Secure Resilient Real-Time Recovery Model, Scheduler, and Analysis*' in 10th International Workshop on Mixed Criticality Systems **(RTSS-WMC)**, 2022.

AWARDS AND SCHOLARSHIPS

Graduate Merit Award (NCSU)	2024
Mentored Teaching Fellowship (NCSU)	Spring 2024
DAC 2022 Publicity Paper	2022
Doctoral Research Support Award (UCF)	2021
ORC Fellowship (UCF)	2018
Runner-Up (Cadence DSP Design Contest)	2016
CPS-IoT Week Student Travel Grant	2023 (SIGBED); 2024 (NSF)
COE Student Travel Grant (NCSU)	2023
RTSS Student Travel Grant	2022 (IEEE)
Presentation Fellowship (UCF)	2022

PRESENTATIONS AND TALKS

Fisher Information Guided Purification against Backdoor Attacks (CCS)	2024
Dynamic Priority Scheduling of Multi-Threaded ROS 2 Executor with Shared Resources (EMSOFT)	2024

Compositional Mixed-Criticality Systems with Multiple Executions and Resource-Budgets Model (RTAS) 2023

A Secure Resilient Real-Time Recovery Model, Scheduler, and Analysis (WMC) 2022

Response Time Analysis for Dynamic Priority Scheduling in ROS2 (IEEE/ACM DAC) 2022

VR-Spy: A Side-Channel Attack on Virtual Key-Logging in VR Headsets (IEEE VR) 2021

SKILLS

Programming	Python, C/C++, MATLAB
Verification Tools	UPPAAL
Real-Time OS	ROS 2, FreeRTOS, LinuxRT

MENTORING EXPERIENCE

Kurt Wilson, Ph.D. Student at North Carolina State University
Publications: DAC'22 [**Publicity Paper Award**], EMSOFT'24

Srishti Swarnima, MS Student at North Carolina State University

PROFESSIONAL SERVICES

Reviewer

IEEE Internet of Things Journal (IoT-J)	2023
AAAI Conference on Artificial Intelligence (AAAI)	2024
International Conference on Real-Time Networks and Systems (RTNS)	2021, 2022, 2023
Embedded and Real-Time Computing Systems and Applications (RTCSA)	2021, 2022, 2023

Secondary Reviewer 2021 - 2024

Journals

IEEE IoT-J, IEEE TNNLS, IEEE TCAD, IEEE TIME, IEEE TPDS, ACM TECS, etc.

Conferences

Real-Time Systems Symposium (**RTSS** 2021, 2022, 2023, 2024)
ACM SIGBED International Conference on Embedded Software (**EMSOFT** 2024)
Euromicro Conference on Real-Time Systems (**ECRTS** 2024)
Real-Time and Embedded Technology and Applications (**RTAS** 2022, 2024)
Design Automation Conference (**DAC** 2021, 2022)

REFERENCES

Zhishan Guo
Associate Professor, North Carolina State University
Phone: 919-515-3962
Email: zguo32@ncsu.edu