HABIBA FARRUKH

305 N University Street, West Lafayette, IN, 47907
hfarrukh@purdue.edu ◇ https://habiba-farrukh.github.io/ ◇ (765) 479-9736

EDUCATION

Purdue University **2017 - Present**

- Ph.D. in Computer Science
- Advisor: Professor Z. Berkay Celik
- Thesis: Leveraging Multi-modal Sensing for Improving Mobile Systems Security & Privacy

LUMS School of Science & Engineering, Pakistan **2012 - 2016**

- B.S. in Computer Science (*summa cum laude*)

RESEARCH AND PROFESSIONAL EXPERIENCE

Lead Graduate Student - Prof. Celik's Research Group, Purdue University 2021 - Present

- Conduct project meetings with the five graduate students
- Provide students with mentoring and research guidance

Research Assistant - Purdue University **2017 - Present**

- Designed secure and usable camera-based liveness detection system for commodity mobile devices
- Investigated sensor-based attacks on mobile devices
- Introduced secure group pairing system for IoT devices
- Investigated technology abuse and its impact on vulnerable populations
- Disseminated research through academic conference papers

Applied Scientist Intern - Amazon Robotics **2020**
Hosted by Tim Stallman in Machine Learning Science Team

- Conducted research on improving effectiveness of robotic package identification systems
- Developed a deep-learning based automated package identification system for robotic arms in Amazon's fulfillment centers

Research Assistant - Network and Systems Group, LUMS **2015 - 2016**
Mentored by Prof. Ihsan Ayyub Qazi

- Redesigned switch buffer organization scheme for data centers.
- Developed software defined networks for separating data flows, managing buffer sizes and handling weighted processor sharing.

AWARDS AND HONORS

- Bilsland Dissertation Fellowship Award, awarded by the Dean of the Graduate School to support outstanding Ph.D. candidates (2022)
- ACM CCS Student Travel Grant (2022)
- Student Lead of Google ASPIRE Award "Improving the Security and Usability of the Wear OS Permission Model" (2022)
- Student Lead of Google ASPIRE Award "Improving Usability of Android APIs for Conformity of Standard Security Practices" (2021)
- NSF Student Travel Grant from ACM MobiSys (2018)
- Grace Hopper Conference for Women in Computing Scholarship (2018)
- Graduation with Distinction (Bachelor of Science)
- Dean's Honor List (2014 – 2016)

PROFESSIONAL ACTIVITIES

Program Committee Member

- USENIX Security Symposium, 2023
- ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2023
- ACM Wireless of the Students, by the Students, and for the Students (S^3) Workshop (co-located with MobiCom), 2021

Reviewer

- ACM Transactions on Sensor Networks (TOSN), 2022
- ACM Computing Surveys (CSUR), 2022

External Reviewer

- Network and Distributed System Security (NDSS), 2023
- USENIX Security Symposium, 2022
- Annual Computer Security Applications Conference (ACSAC), 2021
- Network and Distributed System Security (NDSS), 2021

TEACHING EXPERIENCE

Guest Lecturer

- CS590 IoT & CPS Security, Purdue University, Spring 2022
  Topic: Side Channel Attacks: Definition, Attack Types, Threat Models

Teaching Assistant

- CS422 Computer Networks, Purdue University, Fall 2020
- CS422 Computer Networks, Purdue University, Fall 2019
- CS422 Computer Networks, Purdue University, Spring 2018
- CS251 Data Structures and Algorithms, Purdue University, Fall 2017
- CS251 Data Structures and Algorithms, Purdue University, Spring 2017

STUDENT RESEARCH ADVISING

Haozhe Zhou	B.S. Computer Science, Purdue University → Ph.D. CMU	2021-2022
Eliz Teckan	M.S. Computer Science, Purdue University → Vestel	2021-2022
Aniket Nare	M.S. Computer Science, Purdue University → Amazon	Summer 2022
Jason Perry	B.S. Computer Science, Purdue University (exp. 2022)	2020-2022
Hanwen Xu	B.S. Computer Science, Tsinghua University	2019
Yuxuan Lin	B.S. Computer Science, Tsinghua University	2019

PUBLICATIONS

Conference Publications

C1 **Habiba Farrukh**[*], Muslum Ozgur Ozmen[*], Faik Kerem Ors, and Z. Berkay Celik
Secure Group Pairing for Heterogeneous IoT Devices,
Proceedings of the IEEE Security and Privacy (S&P), 2023.

C2 Reham Mohamed Aburas, **Habiba Farrukh**, He Wang, Yidong Lu, and Z. Berkay Celik
Disclosing Sensitive User Information by Mobile Magnetometer from Finger Touches,
Privacy Enhancing Technologies (PoPETs), 2023.

C3 Muslum Ozgur Ozmen, Ruoyu Song, **Habiba Farrukh**, and Z. Berkay Celik
Evasion Attacks on Smart Home Physical Event Verification and Defenses
Proceedings of the Network and Distributed System Security Symposium (NDSS), 2023. (Acceptance Rate: 19%)

C4 Abdullah Imran, **Habiba Farrukh**, Muhammad Ibrahim, Z. Berkay Celik, and Antonio Bianchi
SARA: Secure Android Remote Authorization
Proceedings of the USENIX Security Symposium, 2022. (Acceptance Rate: 17%)

C5 Siddharth Divi, Yi-Shan Lin, **Habiba Farrukh**, and Z. Berkay Celik
New Metrics to Evaluate the Performance and Fairness of Personalized Federated Learning
International Workshop on Federated Learning for User Privacy and Data Confidentiality, co-located with International Conference on Machine Learning (ICML), 2021.

C6 **Habiba Farrukh**, Tinghan Yang, Hanwen Xu, Yuxuan Yin, He Wang, and Z. Berkay Celik
S^3: Side-channel attack on Stylus Pencils through Sensors
Proceedings of the ACM Interactive, Mobile, Wearable and Ubiquitous Technologies (IMWUT /UbiComp), 2021.

C7 **Habiba Farrukh**, Reham Aburas, Siyuan Cao, and He Wang
FaceRevelio: A Face Liveness Detection System for Smartphones with a Single Front Camera
Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom), 2020. (Acceptance Rate: 16%)

C8 Siyuan Cao, **Habiba Farrukh**, and He Wang
Towards Context Address for Camera-to-Human Communication
Proceedings of the IEEE International Conference on Computer Communications (InfoCom), 2020. (Acceptance Rate: 19%)

C9 Siyuan Cao, **Habiba Farrukh**, and He Wang
Demo: Enabling Public Cameras to Talk to the Public
Proceedings of the ACM International Conference on Mobile Systems, Applications, and Services (MobiSys), 2018.

Papers in Review

S1 **Habiba Farrukh**, Reham Mohamed Aburas, Aniket Nare, Antonio Bianchi, and Z. Berkay Celik
Inferring Semantic Location from Spatial Maps in Mixed Reality, 2022.

S2 Arjun Arunasalam*, **Habiba Farrukh*** and Eliz Tekcan*, and Z. Berkay Celik
Understanding the Security and Privacy Implications of Online Toxic Content on Refugees, 2022.

$*$ denotes equal contribution

PATENTS

P1 Siyuan Cao, **Habiba Farrukh**, He Wang
Method of communicating between a client-server system and remote clients, US Patent 11,030,869.

P2 **Habiba Farrukh**, Reham Mohammed, Siyuan Cao, He Wang
System architecture and method of authenticating a 3D object, US Patent App.

16819166.

REFERENCES

Z. Berkay Celik
Assistant Professor, CS department, Purdue University
Email: zcelik@purdue.edu
Phone: (765) 496-1761

Antonio Bianchi
Assistant Professor, CS department, Purdue University
Email: antoniob@purdue.edu
Phone: (765) 494-7100

Dongyan Xu
Professor, CS department, Purdue University
Director of CERIAS
Email: dxu@purdue.edu
Phone: (765) 494-6182