MD HAFIZUL CHOWDHURYY

Phone: +14076843839
Email: hafizul.islam@ucf.edu

BIOGRAPHY

My primary research area is at the intersection of computer architecture and security, focusing on the development of secure and high-performance microarchitectural systems and emerging memory architectures. My work has led to the identification of new vulnerabilities in modern CPU microarchitecture and secure processors, exploiting real-world cryptographic applications and machine learning workloads. Additionally, I have designed and implemented secure-by-design architectural solutions. I have published as first author in many prestigious venues, including all three top-tier architecture conferences (ISCA, MICRO, and HPCA) and the Systems Security Conference (S&P).

EDUCATION

PhD in Computer Engineering
University of Central Florida
Year: Fall'2019 – Summer'2024

M.Sc. in Electrical and Electronic Engineering
University of Chittagong
Passing year: 2019

B.Sc. in Electrical and Electronic Engineering
University of Chittagong
Passing year: 2017

PUBLICATIONS

Peer-review Conferences

- [**MICRO'24**] Md Hafizul Chowdhuryy and Fan Yao, *IvLeague: Side Channel-resistant Secure Architectures Using Isolated Domains of Dynamic Integrity Trees*, In IEEE/ACM International Symposium on Microarchitecture, 2024. (*Top-tier Conference*)
- [**ISCA'24**] Md Hafizul Chowdhuryy, Hao Zheng and Fan Yao, *MetaLeak: Uncovering Side Channels in Secure Memory Architectures Exploiting Metadata*, In IEEE/ACM Annual International Symposium on Computer Architecture, 2024. (*Top-tier Conference*)
- [**S&P'24**] Kunbei Cai, Md Hafizul Chowdhuryy, Zhenkai Zhang and Fan Yao, *DeepVenom: Persistent DNN Backdoors Exploiting Transient Weight Perturbations*, In IEEE Symposium on Security and Privacy, 2024. (*Top-tier Conference*)
- [**AsiaCCS'24**] Md Hafizul Chowdhuryy, Zhenkai Zhang and Fan Yao, *PowSpectre: Powering Up Speculation Attacks with TSX-based Replay*, In ACM ASIA Conference on Computer and Communications Security, 2024.
- [**ICCAD'23**] Md Hafizul Chowdhuryy, Zhenkai Zhang and Fan Yao, *BeKnight: Guarding against Information Leakage in Speculatively Updated Branch Predictor*, In IEEE/ACM International Conference on Computer-Aided Design, 2023. (*Top-tier Conference*)
- [**HPCA'23**] Md Hafizul Chowdhuryy, Myoungsoo Jung, Fan Yao and Amro Awad, *D-Shield: Enabling Processor-side Encryption and Integrity Verification for Secure NVMe Drives*, In IEEE International Symposium on High-Performance Computer Architecture, 2023. (*Top-tier Conference*)
- [**S&P'22**] Md Hafizul Chowdhuryy+, Adnan Siraj Rakin+, Fan Yao and Deliang Fan (+Co-first authors), *DeepSteal: Advanced Model Extractions Leveraging Efficient Weight Stealing in Memories*, In IEEE Symposium on Security and Privacy, 2022. (*Top-tier Conference*)
- [**MICRO'21**] Md Hafizul Chowdhuryy, Muhammad R. Haq Rashed, Amro Awad, Rickard Ewetz and Fan Yao, *LADDER: Architecting Content and Location-aware Writes for Crossbar Resistive Memories*, In IEEE/ACM International Symposium on Microarchitecture, 2022. (*Top-tier Conference*)
- [**SEED'21**] Md Hafizul Chowdhuryy, Rickard Ewetz, Amro Awad and Fan Yao, *R-SAW: New Side Channels Exploiting Read Asymmetry in MLC Phase Change Memories*, In IEEE International Symposium on Secure and Private Execution Environment Design, 2021.
- [**SEED'21**] Kunbei Cai, Md Hafizul Chowdhuryy, Zhenkai Zhang and Fan Yao, *NMT-Stroke: Diverting Neural Machine Translation through Hardware-based Faults*, In IEEE International Symposium on Secure and Private Execution Environment Design, 2021.
- [**ICCD'20**] Md Hafizul Chowdhuryy, Hang Liu and Fan Yao, *BranchSpec: Information Leakage Attacks Exploiting Speculative Branch Instruction Executions*, In IEEE International Conference on Computer Design, 2020.

Journals

- [**Micro'23**] Md Hafizul Chowdhuryy, Rickard Ewetz, Amro Awad and Fan Yao, *Understanding and Characterizing Side Channels Exploiting Phase Change Memories*, In IEEE Micro, 2023.
- [**TC'21**] Md Hafizul Chowdhuryy and Fan Yao, *Leaking Secrets through Modern Branch Predictor in the Speculative World*, In IEEE Transactions on Computers, 2021.

ACADEMIC SERVICES

1. IEEE Transactions on Computers (2022,2023) – Reviewer.
2. IEEE International Conference on Computer Design (2023) – Publicity chair.
3. IEEE Transactions on Dependable and Secure Computing (2022,2023) – Reviewer.
4. Design Automation Conference (2023) – Sub-reviewer.
5. IEEE International Conference on Networking, Architecture, and Storage (2022) – Sub-reviewer.
6. IEEE International Symposium on Secure and Private Execution Environment Design (2022) – Sub-reviewer.
7. IEEE International Symposium on Workload Characterization (2021) – Artifact Evaluation Committee Member.
8. IEEE International Conference on Computer Design (2021,2022) – Sub-reviewer.

INVITED TALKS/PRESENTATIONS

1. Talk (University of Delaware, 2022): Feasibility and Implication of Remote In-Memory Data Stealing.
2. Presentation (ICCAD'23): BeKnight: Guarding against Information Leakage in Speculatively Updated Branch Predictor.
3. Presentation (HPCA'23): D-Shield: Enabling Processor-side Encryption and Integrity Verification for Secure NVMe Drives.
4. Presentation (S&P'22): DeepSteal: Advanced Model Extractions Leveraging Efficient Weight Stealing in Memories.
5. Presentation (MICRO'21): LADDER: Architecting Content and Location-aware Writes for Crossbar Resistive Memories.
6. Presentation (SEED'21): R-SAW: New Side Channels Exploiting Read Asymmetry in MLC Phase Change Memories.
7. Presentation (ICCD'20): BranchSpec: Information Leakage Attacks Exploiting Speculative Branch Instruction Executions.

TEACHING EXPERIENCE

Introduction to Computer Engineering (**EEL 3801C**) – Summer'23, University of Central Florida (Lab Teaching Assistant).

Hardware Security and Trusted Circuit Design (**EEE 4346C**) – Fall'22/Fall'20, University of Central Florida (Lab Teaching Assistant).

Embedded Systems (**EEL 4742C**) – Spring'21, University of Central Florida (Lab Teaching Assistant).

AWARDS

1. UCF Presentation Fellowship (Fall'2023,Spring'2023,Summer'2022).
2. NSF-sponsored student travel grant award (Spring'2023).
3. IEEE S&P Student Travel Grant (2022).
4. Student Government International Students Scholarship (2021).
5. ORCGS Doctoral Fellowship (2019).

REFERENCES

Dr. Fan Yao, University of Central Florida. **E:** fan.yao@ucf.edu
Dr. Hao Zheng, University of Central Florida. **E:** hao.zheng@ucf.edu
Dr. Yan Solihin, University of Central Florida. **E:** yan.solihin@ucf.edu
Dr. Amro Awad, North Carolina State University. **E:** ajawad@ncsu.edu