Mohamed (Tarek Ibn Ziad) Hassan

Contact Information

42 Wellman Street, Lowell, MA, 01851, USA.
https://www.cs.columbia.edu/∼mtarek/ 1-929-202-3609
https://github.com/TarekIbnZiad mtarek@nvidia.com

Research Interests

Computer security, hardware security, computer architecture, enhancing privacy and system performance via hardware support, and FPGA prototyping.

Education

Fu Foundation School of Engineering and Applied Science, Columbia University, New York, NY, USA

Ph.D. in Computer Science, May 2022
Thesis: Hardware-Software Co-design for Practical Memory Safety

Fu Foundation School of Engineering and Applied Science, Columbia University, New York, NY, USA

M.Phil. in Computer Science, May 2020

Fu Foundation School of Engineering and Applied Science, Columbia University, New York, NY, USA

M.Sc. in Computer Engineering, May 2019
GPA: 4.00/4.00

Faculty of Engineering, Ain Shams University (ASU), Cairo, Egypt

M.Sc. in Computer and Systems Engineering, June 2017
GPA: 3.97/4.00
Thesis: Homomorphic Encryption for Secure Data Computations

Faculty of Engineering, Ain Shams University, Cairo, Egypt

B.Sc. in Computer and Systems Engineering, July 2014
Degree: Excellent with honors Ranking: 1st of class (100 students)
GPA: 4.00/4.00

Awards & Honors

- Won a Qualcomm Innovation Fellowship (QIF North America 2020) for my proposal, "Practical Security for Heterogeneous Systems". Aug. 2020
- Was recognized with an IEEE Micro Top Picks Honorable Mention for my work on fine grained memory safety, Califorms. Jan. 2020
- Selected as an RSAC Security Scholar, which is a nomination-based program for cyber security students to present their work at the RSA Conference. March 2019
- Won the 2nd rank in the TIEC Gradation Project Competition (IBTIECAR 2014) for my B.Sc. Graduation Project, "Acceleration of Numerical Solutions of Differential Equations Using FPGA-Based Emulation Technology". Feb. 2015
- Had the 1st rank, out of 2500 students, graduated on 2014 from the Faculty of Engineering, Ain Shams University, Egypt. I have been honored by the Egyptian president, at the Sixty-fifth Science Festival. July 2014
- Received the Egyptian Government Award for Excellence in Undergraduate Studies, Five years in a row, Ain Shams University. 2009 - 2014
- Won the best semester project award sponsored by Mentor Graphics Egypt. The project requires using Mentor tools to design and implement a simple processor (complete design files, sample test bench and synthesize report). Feb. 2013

Work Experience

Research Scientist at NVIDIA Research June 2022 to present

Joined the Architecture Research Group. Working on the design and implementation of software/hardware techniques for enhancing GPU security.

Graduate Research Assistant at Columbia University Sept. 2017 to May 2022

Served as teaching assistant and grader for the following courses:

- CSEEW4824: Computer Architecture [*Fall 2019*]
- COMSE6424: Hardware Security [*Fall 2018*]

Worked at the Computer Architecture and Security Technologies Lab (CASTL).

- Designed and implemented a software/hardware solution, No-FAT, for lightweight memory safety checks with no metadata.
- Designed and implemented a cohesive solution, SPAM, to mitigate software- and hardware-based memory vulnerabilities.
- Designed a novel technique, PAS, to mitigate code-reuse attacks in resource constrained devices (e.g., IoT devices) using minimal hardware adjustments with no software changes.
- Performed the microarchitecture design and implementation of a novel cache line formatting scheme, Califorms, which provides intra-object protection with low performance overheads compared to existing work.
- Performed the control-theory analysis for a practical technique, YOLO, which aims at increasing the resiliency of Cyber-Physical Systems against software attacks.
- Investigated novel power-based techniques to prevent Hardware Trojans insertion during both design-time and fabrication.

Summer Intern at NVIDIA Research June 2021 to Aug. 2021

Joined the Architecture Research Group and was responsible for the design and implementation of compiler and hardware based memory safety solutions on GPUs.

Summer Intern at QPSI, Qualcomm Inc June 2020 to Aug. 2020

Worked with the Systems Security and Research Team and was responsible for:

- Characterizing code gadgets on the Qualcomm Hexagon processor and evaluating current & potential mitigations.
- Analyzing the security of the Audio framework on current Hexagon DSPs.

Teaching Assistant at Faculty of Engineering, ASU Aug. 2014 to July 2017

Served as teaching assistant and grader for the following courses:

- CSE011: Computer Technology
- CSE121: Computer Programming
- CSE128: Software Engineering (1)
- CSE222: Software Engineering (2)
- CSE211: Computer Organization (1)
- CSE271: System Dynamics and Control Components
- CSE351: Electrical Testing (2)
- CSE431: Computer Networks
- CSE451: Electrical Testing (3)

Software Development Engineer, Mentor Graphics Feb. 2016 to July 2017

Joined the Hardware Modeling Team of Virtual Platforms and was responsible for:

- Developing software Models for Hardware devices using Vista tools.
- Creating SystemC TLM 2.0 models that can be used to create Virtual Platforms.

- Applying unit testing/debug.

Summer Intern at MED, Mentor Graphics July 2013 to Sept. 2013

Designed and implemented a hardware-based solution to accelerate the Finite Element Method computations using Matlab system generator and Xilinx FPGA boards.

Technical Skills

Programming Languages	C/C++, CUDA, Java, SystemC.
HDL Languages	Verilog HDL, VHDL.
Scripting Languages	Python, Perl, Tcl.
Hardware	FPGA, Mentor hardware emulators (Veloce), HCS12.
Compiler	Clang/LLVM.
EDA Tools	Synopsys Design Tools, Xilinx ISE Design Suite, ModelSim, Quartus, Code Warrior.
Simulation Tools	Gem5, Matlab/Simulink, CST, Multisim.

Journal Publications

1. **M. Tarek Ibn Ziad**, M. Hossam, M. A. Masoud, M. Nagy, H. A. Adel, Y. Alkabani, M. W. El-Kharashi, K. Salah, and M. AbdelSalam. "On Kernel Acceleration of Electromagnetic Solvers via Hardware Emulation", *Computers and Electrical Engineering*, Volume 47, October 2015, Pages 96–113.

Conference Publications

ArXiv Pre-prints

1. **Mohamed Tarek Ibn Ziad**, Miguel A. Arroyo, and Simha Sethumadhavan. "SPAM: Stateless Permutation of Application Memory", *Technical Report*, September 2020.

2. **Mohamed Tarek Ibn Ziad**, Miguel A. Arroyo, Evgeny Manzhosov, Vasileios P. Kemerlis, and Simha Sethumadhavan. "Using Name Confusion to Enhance Security", *Technical Report*, August 2020.

Accepted Papers

1. Evgeny Manzhosov, Adam Hastings, Meghna Pancholi, Ryan Piersma, **Mohamed Tarek Ibn Ziad** and Simha Sethumadhavan. "Revisiting Residue Codes for Modern Memories", *In the Proceedings of the 55th IEEE/ACM International Symposium on Microarchitecture (MICRO-55)*, Chicago, IL, USA, October 2022.

2. **Mohamed Tarek Ibn Ziad**, Miguel A. Arroyo, Evgeny Manzhosov, Vasileios P. Kemerlis, and Simha Sethumadhavan. "EPI: Efficient Pointer Integrity For Securing Embedded Systems", *In the Proceedings of the 2021 IEEE International Symposium on Secure and Private Execution Environment Design (SEED '21)*, Worldwide Event, September 2021.

3. **Mohamed Tarek Ibn Ziad**, Miguel A. Arroyo, Evgeny Manzhosov, and Simha Sethumadhavan. "ZeRØ: Zero-Overhead Resilient Operation Under Pointer Integrity Attacks", *In the Proceedings of the 48th International Symposium on Computer Architecture (ISCA-48)*, Worldwide Event, June 2021.

4. **Mohamed Tarek Ibn Ziad**, Miguel A. Arroyo, Evgeny Manzhosov, R. Piersma, and Simha Sethumadhavan. "No-FAT: Architectural Support for Low Overhead Memory Safety Checks", *In the Proceedings of the 48th International Symposium on Computer Architecture (ISCA-48)*, Worldwide Event, June 2021.

5. Hiroshi Sasaki, Miguel A. Arroyo, **M. Tarek Ibn Ziad**, Koustubha Bhat, Kanad Sinha, and Simha Sethumadhavan. "Practical Byte-Granular Memory Blacklisting using Califorms", *In the Proceedings of the 52nd IEEE/ACM International Symposium on Microarchitecture (MICRO-52)*, Columbus, Ohio, USA, October 2019.
6. Miguel A. Arroyo, **M. Tarek Ibn Ziad**, Hidenori Kobayashi, Junfeng Yang, and Simha Sethumadhavan. "YOLO: Frequently Resetting Cyber-Physical Systems for Security", *In the Proceedings of the SPIE Defense and Commercial Sensing*, Baltimore, Maryland, USA, April 2019.
7. **M. Tarek Ibn Ziad** and Simha Sethumadhavan. "Subtractive Hardware Trojans", *In RSA Conference Poster Session*, San Francisco, CA, USA, March 2019.
8. **M. Tarek Ibn Ziad**, Amr Alanwar, Moustafa Alzantot, and Mani Srivastava. "CryptoImg: Privacy Preserving Processing Over Encrypted Images", *In the Proceedings of the 2nd IEEE Workshop on Security and Privacy in the Cloud (SPC), held in conjunction with the IEEE Conference on Communications and Network Security (CNS)*, Philadelphia, PA, USA, October 2016.
9. **M. Tarek Ibn Ziad**, Y. Alkabani, M. W. El-Kharashi, K. Salah, and M. Abdel-Salam. "Accelerating Electromagnetic Simulations: a Hardware Emulation Approach", *In Proceedings of the 2015 IEEE International Conference on Electronics Circuits, and Systems (ICECS)*, pages 592–595, Cairo, Egypt, December 2015.
10. **M. Tarek Ibn Ziad**, Y. Alkabani, and M. W. El-Kharashi. "On Hardware Solution of Dense Linear Systems via Gauss-Jordan Elimination", *In Proceedings of the 2015 IEEE Pacific Rim Conference on Communications, Computers, and Signal Processing (PacRim)*, pages 364–369, Victoria, B.C., Canada, August 2015.
11. **M. Tarek Ibn Ziad**, A. Al-Anwar, Y. Alkabani, M. W. El-Kharashi, and H. Bedour. "Homomorphic Data Isolation for Hardware Trojan Protection", *In Proceedings of the IEEE Computer Society Annual Symposium on VLSI (ISVLSI 2015)*, pages 131–136, Montpellier, France, July 2015.
12. **M. Tarek Ibn Ziad**, M. Hossam, M. A. Masoud, M. Nagy, H. A. Adel, Y. Alkabani, M. W. El-Kharashi, K. Salah, and M. AbdelSalam. "Finite Element Emulation-based Solver for Electromagnetic Computations", *In Proceedings of the 2015 IEEE International Symposium on Circuits and Systems (ISCAS)*, pages 1434–1437, Lisbon, Portugal, May 2015.
13. **M. Tarek Ibn Ziad**, A. Al-Anwar, Y. Alkabani, M. W. El-Kharashi, and H. Bedour. "E-Voting Attacks and Countermeasures". *In the Proceedings of the 10th International Symposium on Frontiers of Information Systems and Network Applications (FINA 2014), held in conjunction with the 28th IEEE International Conference on Advanced Information Networking and Applications (AINA-2014)*, pages 269–274, Victoria, BC, Canada, May 2014.

Patents

1. Methods & Systems for Fine Granularity Memory Blacklisting to Detect Memory Access Violations, Application No. US 16/744922, Simha Sethumadhavan, Hiroshi Sasaki, **Mohamed Tarek Ibn Ziad**, and Miguel A. Arroyo, 2019.
2. Control Flow Protection Based on Phantom Addressing, Application No. US 17/030785, Simha Sethumadhavan, Miguel A. Arroyo, **Mohamed Tarek Ibn Ziad**, and Evgeny Manzhosov, 2019.

Work In Progress

1. **Mohamed Tarek Ibn Ziad** and Simha Sethumadhavan. "Hardware Support For Memory Safety", *Synthesis Lectures on Computer Architecture.*
2. **Mohamed Tarek Ibn Ziad**, Evgeny Manzhosov, and Simha Sethumadhavan. "C-4: Compromising Cryptographic Capability Computing".
3. **Mohamed Tarek Ibn Ziad**, Evgeny Manzhosov, Ryan Piersma, and Simha Sethumadhavan. "STOPS: Speculation-Throttling Operation For Secrets".

Research Talks

ZeRØ: Zero-Overhead Resilient Operation Under Pointer Integrity Attacks

- International Symposium on Computer Architecture (ISCA), Virtual. June 2021
- Symposium on Hot Topics in the Science of Security (HotSoS), Virtual. April 2021

No-FAT: Architectural Support for Low Overhead Memory Safety Checks

- NVIDIA Research, Virtual. July 2021
- International Symposium on Computer Architecture (ISCA), Virtual. June 2021

Practical Byte-Granular Memory Blacklisting using Califorms

- Qualcomm Product Security Group, Virtual. August 2020
- International Symposium on Microarchitecture, Columbus, OH, USA. Oct. 2019

Using Name Confusion to Enhance Security

- International Symposium on Secure and Private Execution Environment Design (SEED), Virtual. September 2021
- Qualcomm Product Security Group, Virtual. August 2020

SPAM: Stateless Permutation of Application Memory

- LLVM Developers' Meeting, Virtual. October 2020

Systems Security: Why is Memory Safety Still a Concern?

- Columbia University, Virtual. February 2021
- PhD Candidacy Presentation, Virtual. April 2020

YOLO: Frequently Resetting Cyber-Physical Systems for Security

- International Workshop on the Design and Analysis of Robust Systems (DARS), New York, NY, USA. July 2019

Academic Service

- Technical Conference Reviewer: ISCA 2021, S&P 2021, ISVLSI 2020.
- Technical Journal Reviewer: IEEE Transactions on Computer Aided Design of Integrated Circuits & Systems, IEEE Transactions on Computers, IEEE Computer Architecture Letters.
- Program-Committee Member: IEEE Security & Privacy (Oakland) 2023.
- External Program-Committee Member: ASPLOS 2023.

Soft Skills

- Self-motivated and able to work independently.
- Team leader.
- Good written and verbal communication skills.
- Time management.

References

Simha Sethumadhavan
Professor of Computer Science, Columbia University
simha@columbia.edu

Vasileios P. Kemerlis
Assistant Professor of Computer Science, Brown University
vpk@cs.brown.edu

Aamer Jaleel
Principal Research Scientist, Architecture Research Group, Nvidia Research
ajaleel@nvidia.com