Youssef Tobah

703-505-1178 |ytobah@umich.edu

Education

PhD, Computer Science and Engineering **Dec 2024**
Kang G. Shin
University of Michigan

Master of Science, Computer Science and Engineering **May 2020**
University of Michigan

Bachelor of Science, Electrical Engineering **May 2018**
The University of Texas at Austin
Overall GPA: 3.96/4.00

Selected Publications

1. **Youssef Tobah,** Ingab Kang, Andrew Kwong, Daniel Genkin, Kang G. Shin, "Go Go Gadget Hammer: Flipping Nested Pointers for Arbitrary Data Leakage," *USENIX Security '24.*

2. Ingab Kang, Walter Wang, Jason Kim, Stephan van Schaik, **Youssef Tobah**, Daniel Genkin, Andrew Kwong, and Yuval Yarom, "SledgeHammer: Amplifying Rowhammer via Bank-level Parallelism," *USENIX Security '24.*

3. **Youssef Tobah,** Ingab Kang, Andrew Kwong, Daniel Genkin, Kang G. Shin, "SpecHammer: Combining Spectre and Rowhammer for new speculative attacks," *IEEE S&P'22.* (Impact score: 1.17)

4. Aydin Aysu, **Youssef Tobah,** Mohit Tiwari, Andreas Gerstlauer, Michael Orshansky, "Horizontal side-channel vulnerabilities of post-quantum key exchange protocols," *HOST'18.* (Impact score: 3.02)

5. Deepika Yadav, **Youssef Tobah,** Kenta Sugawara, Junki Mitsushio, Gen Tamamushi, Takayuki Watanabe, Alexander A. Dubinov, Victor M. Ryzhii, Taiichi Otsuji. "Terahertz light emitting transistor based on current injection dualgate graphene-channel FET," *IRMMW-THz 2017.* (Impact score: 0.42)

Work Experience

Intern, MIT Lincoln Laboratory, Boston, Massachusetts 6/22 – 8/22

- Reverse engineered physical-to-DRAM address mapping on latest Intel processors
- Physically probed DRAM using oscilloscope to obtain ground truth mapping
- Used timing side-channel to obtain mapping via software techniques (using code written in C)
- Induced first Rowhammer bitflips on an Intel Generation 12 processor

Intern, Hara Laboratory, Tokyo Institute of Technology, Tokyo, Japan 6/18 – 8/18

- Researched single instruction computing for low-power, small-area embedded systems
- Executed area and power reduction techniques for four-instruction processor
- Implemented single instruction architecture in Verilog
- Reduced energy costs to 50% and area costs to 25%

Undergraduate Assistant Researcher, The University of Texas at Austin 2/16 – 11/17

- Wrote Python scripts in Linux for automating benchmark annotation process
- Modified machine learning programs to approximate computations and save power during runtime
- Implemented VHDL matrix multiplier for post-quantum cryptography security project

Intern, NASA Goddard Space Flight Center 6/17 – 8/17

- Developed debugging tool for gathering Xilinx microblaze processor performance
- Wrote drivers in C for Linux and FreeRTOS
- Modified VHDL code and debugged on FPGA

Academic Experience

Combined Spectre-Rowhammer Attack Research Project, University of Michigan 9/19 – 8/21

- Developed novel attack enhancing Spectre's capabilities by combining with Rowhammer
- Wrote proof-of-concept C code to grant arbitrary reads on kernel memory
- Implemented new memory massaging techniques to enable bit-flips on kernel stack
- Discovered 20,000 additional points of vulnerability within the kernel's code

ARM Rowhammer Attack Research Project, University of Michigan 9/18 – 12/18

- Developed attack to gain privilege as malicious user on ARM device
- Implemented Rowhammer and page-spray attack
- Programmed in C and implemented in Linux

Wearable RFID Touch Detector Research Project, University of Michigan 9/19 – 12/19

- Designed embedded system to automatically identify objects user touches
- Implemented as small portable device wearable on the wrist
- Combines RFID and machine learning to identify objects based on vibrations caused by touch

"Ghost V.S. Tank" Video Game Project, The University of Texas at Austin 11/16 – 12/16

- Designed, coded, and assembled two-player video game utilizing IR sensors as method of control
- Utilized various features of microcontroller and embedded systems
- Programmed in C and designed system's PCB
- Collaborated as a team to ensure efficiency

Programming Languages

C, C#, Python, Assembly

Accomplishments

Top Pick in Hardware and Embedded Security	5/2021
Award, Smalley-Curl Institute Research Colloquium	8/2016
Member, IEEE Robotics and Automation Society	8/2014 – 12/2015