NADER SEHATBAKHSH

85 5th St NW, Room 416A, Atlanta, GA 30308
Contact: (+1)4044262998 ⋄ nader.sb@gatech.edu
Homepage: http://www.prism.gatech.edu/∼nsehatbakhsh3/

RESEARCH INTERESTS

- Security and Privacy with emphasis on computer architecture, hardware security, and system design,
- Side-Channel Analysis, both physical (power, electromagnetic, etc.) and digital side-channels (timing, cache, transient/speculative execution, etc.),
- Embedded systems, cyber-physical systems, and internet-of-things security,
- Secure and privacy-preserving remote computing with emphasis on machine-learning applications.

EDUCATION

Georgia Institute of Technology *Atlanta, GA, USA*
PhD Computer Science *Aug. 2014 - May 2020 (expected)*
Thesis Title: *"Leveraging Side-Channel Signals for Security and Trust"*
Advisors: Milos Prvulovic and Alenka Zajic

Georgia Institute of Technology *Atlanta, GA, USA*
M.Sc. Electrical Engineering *Aug. 2014 - Dec. 2017*

University of Tehran *Tehran, Iran*
B.Sc. Electrical Engineering *Sept. 2009 - Jun. 2014*

HONORS AND AWARDS

- **Best Paper Award**, 49th IEEE/ACM Symposium on Microarchitecture (MICRO-49), 2016.
- **Best Paper Nominee**, 26th IEEE International Symposium on High-Performance Computer Architecture (HPCA-26), 2020.
- **IEEE Micro Top Picks Honorable Mention**, 2018.
- **Featured Paper**, in the March 2020 issue of IEEE Transactions on Computers.
- **Second Best Demo Award**, IEEE International Symposium on Hardware Oriented Security and Trust (HOST), 2017.
- **Best Student Paper Award**, IEEE Region 8 Student Paper Contest, 2014.
- Named as one of the Georgia Tech's Research **Highlight of the Year**, 2016.

PUBLICATIONS

Conferences:

C8. [**HPCA'20**] *"A New Side-Channel Vulnerability on Modern Computers by Exploiting Electromagnetic Emanations from the Power Management Unit."*
Nader Sehatbakhsh, Berkay Yilmaz, Alenka Zajic, and Milos Prvulovic.
To appear in Proceedings of the 26th IEEE International Symposium on High-Performance Computer Architecture (HPCA-26).
Acceptance Rate: 19.3%.

C7. [**HPCA'20**] *"EMSim: A Microarchitecture-Level Simulation Tool for Modeling Electromagnetic Side-Channel Signals."*
Nader Sehatbakhsh, Berkay Yilmaz, Alenka Zajic, and Milos Prvulovic.
To appear in Proceedings of the 26th IEEE International Symposium on High-Performance Computer Architecture (HPCA-26).
Acceptance Rate: 19.3%.
HPCA Best Paper Nominee.

C6. [**MICRO'19**] *"EMMA: Hardware/Software Attestation Framework for Embedded Systems Using Electromagnetic Signals."*
Nader Sehatbakhsh, Alireza Nazari, Haider Khan, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 52nd IEEE/ACM International Symposium on Microarchitecture (MICRO-52).
Acceptance Rate: 21%.

C5. [**AAAI-FSS'19**] *"Security and Privacy Considerations for Machine Learning Models Deployed in the Government and Public Sector."*
Nader Sehatbakhsh, Ellie Daw, Onur Savas, Amin Hassanzadeh, Ian McCulloh.
(To appear) in Proceedings of the AAAI Conference on Artificial Intelligence, Fall Symposium Series (AAAI-FSS'19).

C4. [**HOST'18**] *"Syndrome: Spectral Analysis for Anomaly Detection on Medical IoT and Embedded Devices."*
Nader Sehatbakhsh, Monjur Alam, Alireza Nazari, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 11th International Symposium on Hardware-Oriented Security and Trust (HOST'18).
Acceptance Rate: 19%.
Second Best Demo Award.

C3. [**ISCA'17**] *"EDDIE: EM-Based Detection of Deviations in Program Execution."*
Alireza Nazari, **Nader Sehatbakhsh** (*same contribution*), Monjur Alam, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 44th International Symposium on Computer Architecture (ISCA'17).
Acceptance Rate: 16%.
Micro Top Picks Honorable Mention.

C2. [**MICRO'16**] *"Spectral Profiling: Observer-Effect-Free Profiling by Monitoring EM Emanations."*
Nader Sehatbakhsh, Alireza Nazari, Alenka Zajic, and Milos Prvulovic.
In Proceedings of the 49th IEEE/ACM International Symposium on Microarchitecture (MICRO-49).
Acceptance Rate: 21%.
MICRO Best Paper Award.

C1. [**DTIS'14**] *"FPGA Implementation of Genetic Algorithm for Dynamic Filter-Bank-Based Multi-carrier Systems."*
Nader Sehatbakhsh Mohammad Aliasgari, and Sied Mehdi Fakhraie.
In Proceedings of the 8th IEEE International Conference on Design and Technologies in Nanoscale Era (DTIS'14).
Acceptance Rate: 29%.
Best Student Paper Award.

Journals:

J6. [**IEEE Transactions on Computers**] *"REMOTE: Robust External Malware Detection Framework by Using Electromagnetic Signals."*

Nader Sehatbakhsh, Alireza Nazari, Monjur Alam, Frank Werner, Yuanda Zhu, Alenka Zajic, and Milos Prvulovic.
DOI: 10.1109/TC.2019.2945767 (2019).
Featured Paper in March 2020 issue.

J5. [**IEEE Transactions on Dependable and Secure Computing**] *"IDEA: Intrusion Detection through Electromagnetic-Signal Analysis for Critical Embedded and Cyber-Physical Systems."*
Haider Khan, **Nader Sehatbakhsh**, Luong N. Nguyen, Robert Callan, Arie Yeredor, Milos Prvulovic, and Alenka Zajic.
DOI: 10.1109/TDSC.2019.2932736 (2019).

J4. [**IEEE Transactions on Information Forensics and Security**] *"Communication Model and Capacity Limits of Covert Channels Created by Software Activities."*
Berkay Yilmaz, **Nader Sehatbakhsh**, Milos Prvulovic, and Alenka Zajic.
DOI: 10.1109/TIFS.2019.2952265 (2019).

J3. [**Journal of Hardware and Systems Security (HASS)**] *"Malware Detection in Embedded Systems using Neural Network Model for Electromagnetic Side-Channel Signals."*
Haider Khan, **Nader Sehatbakhsh**, Luong N. Nguyen, Milos Prvulovic, and Alenka Zajic.
DOI: 10.1007/s41635-019-00074-w (2019).

J2. [**IEEE Transactions on Antenna and Propagations**] *"A Directive Antenna Based on Conducting Disks for Detecting Unintentional EM Emissions at Large Distances."*
Prateek Juyal, Sinan Adibeli, **Nader Sehatbakhsh**, and Alenka Zajic.
DOI: 10.1109/TAP.2018.2870370 (2018).

J1. [**Elsevier Microelectronics Reliability**] *"PVTA-Aware Approximate Custom Instruction Extension Technique: A Cross-Layer Approach."*
Bahar Farahani, Saeed Safari, and **Nader Sehatbakhsh**.
DOI: 10.1016/j.microrel.2016.05.0080 (2016).

Under Review:

U5. [**HOST'20**] *"SIP: Secure Insertion Policy for Shared Caches to Defeat Conflict-Based Cache Attacks."*
Nader Sehatbakhsh, Moumita Dey, Alenka Zajic, and Milos Prvulovic.
Under Review in the 13th IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'20).

U4. [**S&P'20**] *"SoK: Privacy-Preserving Machine Learning."*
Nader Sehatbakhsh, Ellie Daw, and Amin Hassanzadeh.
Under Review in the 41st IEEE Symposium on Security and Privacy (Oakland, S&P'20).

U3. [**HOST'20**] *"Blind Source Separation of Electromagnetic Side-Channel Signals in Embedded Systems."*
Alireza Nazari, Frank Werner, **Nader Sehatbakhsh**, Alenka Zajic, and Milos Prvulovic.
Under Review in the 13th IEEE International Symposium on Hardware-Oriented Security and Trust (HOST'20).

U2. [**IEEE Transactions on Antenna and Propagation**] *"Side-Channel Propagation Measurements and Modeling for Hardware Security in IoT Devices."*
Seun Sangodoyin, Frank Werner, Baki B. Yilmaz, Chia-Lin Cheng, Elvan M. Ugurlu, **Nader Sehatbakhsh**, Milos Prvulovic, and Alenka Zajic.

Under Review in the IEEE Transactions on Antenna and Propagation (TAP).

U1. [**EuCAP'20**] *"Remote Monitoring and Propagation Modeling of EM Side-Channel Signals for IoT Device Security."*
Seun Sangodoyin, Frank Werner, Baki B. Yilmaz, Chia-Lin Cheng, Elvan M. Ugurlu, **Nader Sehatbakhsh**, Milos Prvulovic, and Alenka Zajic.
Under Review in the 14th European Conference on Antennas and Propagation (EuCAP 2020).

INDUSTRY EXPERIENCE

Accenture Labs — Accenture Cyber-Fusion Center, Washington D.C.
Researcher — *May 2019 - Aug. 2019*

- Explored novel methods for trustworthy AI and privacy-preserving machine learning including designing and implementation of a homomorphic encryption framework.
- Investigated new defense mechanisms against machine-learning privacy attacks (e.g., Membership Inference, Model Extraction, etc.).

Cadence Design Systems — San Jose, CA
Intern — *May 2018 - Aug. 2018*

- Investigated new architectural techniques to improve the performance of a convolutional neural network accelerator using in-house cycle-accurate simulators (C++) and emulators (Python).
- Performed a Power-Performance-Area (PPA) analysis on RISC-V cores to systematically gain insights about the differences between RISC-V and the state-of-the-art ARM and MIPS in-order and OoO cores.

MENTORING EXPERIENCE

Mentored and advised 6 undergraduate students for 3 different year-long projects at the Georgia Institute of Technology (School of ECE) under the "Opportunity Research Scholars" (ORS) program.

- **Hope Hong**, CE, Undergraduate Student, 2017-2019.
  Title of the project: *"Developing a Framework for Defending against Cyber-Security Attacks on Cyber-Physical and Medical Systems."*
  Won the Second Best Demo Award at HOST'18.
- **Oguzhan Yilmaz**, CE, Undergraduate Student, 2017-2019.
  Title of the project: *"'Developing a Framework for Defending against Cyber-Security Attacks on Cyber-Physical and Medical Systems."*
  Won the Second Best Demo Award at HOST'18.
- **Alison Kennedy**, ECE, Undergraduate Student, 2018-2019.
  Title of the project: *"Designing a Secure, Privacy-Preserving Convolutional Neural Network Co-Processor using RISC-V ISA."*
- **Jacob Bruhn**, ECE, Undergraduate Student, 2018-2019.
  Title of the project: *"Designing a Secure, Privacy-Preserving Convolutional Neural Network Co-Processor using RISC-V ISA."*
- **Ben Lazar**, ECE, Undergraduate Student, 2017-2018.
  Title of the project: *"Implementing a Number of Cyber-Attacks (Code-Reuse, Buffer-Overflow, and APT) on Medical Cyber-Physical Devices."*
  Won the Second Best Poster Award at RFID'18.
- **Barry Johnson-Smith**, CE, Undergraduate Student, 2017-2018.
  Title of the project: *"Implementing a Number of Cyber-Attacks (Code-Reuse, Buffer-Overflow, and*

APT) on Medical Cyber-Physical Devices."
Won the Second Best Poster Award at RFID'18.

TEACHING EXPERIENCE

- **TA**, CS 3220 Processor Design (30+ Students), Georgia Tech, Spring'18
- **TA**, CS 6290 Advanced Computer Architecture (50+ Students), Georgia Tech, Fall'16
- **Co-Instructor**, Robotics and Microprocessor Design Lab (30+ Students), University of Tehran Fall'13 & Spring'14
- **TA**, VLSI Design (40+ Students), University of Tehran Spring'13 & Fall'13
- **TA**, Microprocessor Design (60+ Students), University of Tehran Spring'13 & Fall'13

SERVICES

- External Reviewer, *DAC*, 2019.
- Program Committee, *Workshop on Energy Efficient Machine Learning and Cognitive Computing (EMC^2)*, (in conjunction with NeurIPS'19), 2019.
- Reviewer, *IEEE Transactions on Computers*, 2018.
- Reviewer, *IEEE Transactions on Dependable and Secure Computing*, 2019.
- Reviewer, *IEEE Transactions on Circuits and Systems I*, 2019.
- Student Program Committee, *IEEE Symposium on Security and Privacy*, 2018-2019.

TALKS AND PRESENTATIONS

- "EMMA: A Hardware/Software Framework for Establishing Trust on Embedded Systems," International Conference on Microarchitecture, Columbus, OH, 10/19.
- "Leveraging Analog-Domain Side-Channel Signals for Security," Accenture Cyber-Fusion Center, Washington D.C., 7/19.
- "Spectral Analysis for Anomaly Detection on Medical IoT and Embedded Devices," *International Symposium on Hardware-Oriented Security and Trust*, Washington D.C., 5/18.
- "Software Attestation for Embedded Systems Using Electromagnetic Signals," *DARPA review meeting*, Atlanta, GA, 8/18.
- "Robust External Malware Detection Framework by Using Electromagnetic Signals," *DARPA review meeting*. Atlanta, GA, 8/17.

SKILLS

Programming: C/C++, Python, MATLAB, Verilog, x86/ARM Assembly, TCL/Shell scripting, CUDA, MPI, Java.
Software: Virtuoso, Design-Compiler, SoC-Encounter, AVR-Studio, IDA-Pro, Xilinx-ISE, Modelsim.
Hardware Simulators/Tools: gem5, MARSSx86, Intel-Pin, QEMU, SESC, SST-MACSIM, DRAMSIM2, USIMM.
Operating Systems: Linux, MacOS, Windows.
Lab Measurement Tools: Spectrum Analyzer, Oscilloscope, Software-Defined-Radio, Logic Analyzer.

PROFESSIONAL MEMBERSHIPS

ACM, TCCA, IEEE