Arsalan Mosenia

Last update on July 9, 2018

arsalan@princeton.edu • +1-6092162173 • arsalan_m1990 *(Skype)* • https://www.linkedin.com/in/arsalan-mosenia-5b0a6162/ • Department of Electrical Engineering, Princeton University, Princeton, NJ

Summary of Impact

Borrowing concepts from the disciplines of *Information Security, Machine Learning (ML), and Fog/Edge Computing*, my research tackles emerging security and privacy challenges in the Internet-of-Thing (IoT) paradigm. My work has led to the design and development of multiple secure IoT-enabled systems and uncovered fundamental security/privacy flaws in the design of several widely-used systems, including *autonomous vehicles, smartphones, and smart wearables*. My research has resulted in multiple publications in top-tier journals/conferences, *several of which are among the most popular papers of IEEE Transactions*. Furthermore, it has received multiple prestigious awards, including *Princeton Engineering Fellowship, Princeton X Award, Princeton Innovation Award, IP Accelerator Award, Princeton Research Scholarship, and French-American Doctoral Exchange Fellowship* and been featured in several news and media outlets.

Collaboration and Leadership

I have collaborated with over 25 co-authors across 12 industrial research and academic labs. I have mentored and co-supervised over 20 graduate and undergraduate students and led multiple research studies. At OpenFog Consortium, I am actively collaborating with Security Work Group, where we define domain-specific security standards for Fog Computing, and Testbed Work Group, where we design and build novel Fog-inspired systems.

Areas of Expertise

Cyber-physical System Security: Security of Internet-connected/Autonomous Vehicles, Security Analysis of Learning Methods, Security of Smartphones and Smart Wearables, Healthcare Security, and Edge/Fog Security

Privacy-enhancing Technologies: Smartphone Privacy and Healthcare Privacy

Machine Learning (ML): Security Applications of ML, Security Analysis of Deep Learning, and Adversarial ML

Internet of Things (IoT) and Embedded Systems: Fog/Edge Computing, Health Monitoring Systems, Smart Wearables, Internet-connected Cars, and Autonomous Vehicles

Education

Princeton University — Princeton, NJ

Ph.D., Electrical Engineering Department (Computer Engineering Division) — *May 2014 – Jan. 2017*

Thesis: Addressing Security and Privacy Challenges in Internet of Things

Princeton University — Princeton, NJ

M.A., Electrical Engineering Department (Computer Engineering Division) — *Sep. 2012 – May 2014*

Graduate Coursework: Security and Privacy, Machine Learning, Fundamentals of Probability Theory and Random Processes, Information Theory, Surveillance and Countermeasures, Transmission and Compression, Information Security, Electronic Circuits for Biomedical Application, and Very Large-Scale Integrated Circuits

Sharif University of Technology — Tehran, Iran

B.Sc., Computer Engineering Department — *Sep. 2008 – May 2012*

Experience

EDGE Lab, Purdue University — West Lafayette, IN

Postdoctoral Research Scientist — *Jan. 2017 – present*

Host: Mung Chiang

Joint appointment with Princeton

INSPIRE Lab, Princeton University — Princeton NJ

Postdoctoral Research Scientist — *Jan. 2017 – present*

Host: Prateek Mittal

Joint appointment with Purdue

IoT/ML/Security Lab, Princeton University — Princeton NJ

Research Assistant — *May 2012 – Jan. 2017*

Advisor: Niraj Jha

Image Processing Lab (IPL), Sharif University — Tehran Iran
Research Assistant — *May 2011 – May 2012*
Advisor: Shohre Kasaei

Honors and Awards

Intellectual Property Accelerator Award ($100K), Princeton University, 2018
Princeton Innovation Award, Princeton University, 2017
Selected Presenter Award, NJ Tech Council, 2017
French-American Doctoral Exchange Fellowship, 2016 (one of ten selected students in the U.S.)
Project X Award ($100K), Princeton University, 2016
Spotlight paper, IEEE Transactions on Multi-scale Computing Systems (TMSCS), 2015
Princeton Research Scholarship, Princeton University, 2013-2016
Engineering Fellowship, Princeton University, 2012
Talented Student Award, Sharif University of Technology, Iran, 2011 (one of five selected students)

Patents

[1] Secure Optical Communication Channel for Medical Devices [#Publication: US20180109946 A1, 2018]
[2] Continuous Authentication System and Method Based on BioAura [#Publication: US20170230360 A1, 2017]
[3] ProCMotive: Bringing Programability and Connectivity into Isolated Vehicles [U.S. Provisional Patent, 2017]
[4] System and Method for Tracking a Mobile Device User [Provisional Patent (2016), PCT Application (2017)]

Selected Publications

Journal Papers

[1] **A. Mohsen Nia**, M. Mozaffari-Kermani, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "An Energy-efficient System for Long-term Continuous Personal Health Monitoring," IEEE Trans. Multi-scale Computing Systems, Special Issue on Wearables, Implants, and Internet of Things, vol. 1, no. 2, pp. 85–98, 2015 **[recognized as the *spotlight paper*]**
[2] **A. Mohsen Nia**, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Physiological Information Leakage: A New Frontier in Health Information Security," IEEE Trans. Emerging Topics in Computing, vol. 4, no. 3, pp. 321–334, 2016
[3] **A. Mosenia** and N. K. Jha, "A Comprehensive Study of Security of Internet of Thing," IEEE Trans. Emerging Topics in Computing (TETC), vol.5 , no. 4, pp. 586–602, 2017
[4] **A. Mosenia**, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "CABA: Continuous Authentication Based on BioAura," IEEE Trans. Computers, 2017 **[awarded *Project X Award*]**
[5] **A. Mosenia**, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "Wearable Medical Sensor-based System Design: A Survey," IEEE Trans. Multi-Scale Computing Systems, vol. 3, no. 2, pp. 124–138, 2017
[6] **A. Mosenia**, S. Sur-Kolay, A. Raghunathan, and N. K. Jha, "DISASTER: Dedicated Intelligent Security Attacks on Sensor-triggered Emergency Responses," IEEE Trans. Multi-scale Computing Systems, 2017
[7] **A. Mosenia**, X. Dai, P. Mittal, and N. K. Jha, "PinMe: Tracking a Smartphone User around the World," IEEE Trans. Multi-scale Computing Systems, 2017 **[received extensive press coverage]**
[8] **A. Mosenia** and N. K. Jha, "OpSecure: A Secure Unidirectional Optical Channel for Implantable Medical Devices," IEEE Trans. Multi-scale Computing Systems, 2017
[9] Hongxu Yin, Ozge Akmandor, **A. Mosenia**, and N. K. Jha, "Smart Healthcare," Accepted for publication in ACM Foundations and Trends in Electronic Design Automation, 2018

Conference/Workshop Papers

[10] **A. Mosenia**, J. F. Bechara, T. Zhang, P. Mittal, and M. Chiang, "ProCMotive: Bringing Programmability and Connectivity into Isolated Vehicles," ACM Interactive, Mobile, Wearable and Ubiquitous Technologies, will be presented at ACM International Conference on Pervasive and Ubiquitous Computing (Ubicomp), 2018
[11] C. Sitawarin, A. Bhagoji, **A. Mosenia**, P. Mittal, and M. Chiang, "Rogue Signs: Deceiving Traffic Sign Recognition with Malicious Ads and Logos," Deep Learning and Security Workshop at IEEE S&P, 2018
[12] M. Shahrad, **A. Mosenia**, Lewei Song, D. Wentzlaff, M. Chiang, and P. Mittal, "Artesian: Acoustic Denial of Service Attacks on Hard Disk Drives," Submitted to ACM Conference on Computer and Communications Security, 2018 **[received extensive press coverage]**
[13] C. Sitawarin, A. Bhagoji, **A. Mosenia**, P. Mittal, and M. Chiang, "DARTS: Deceiving Autonomous Cars with Toxic Signs," To be submitted to IEEE Symposium on Security and Privacy, Aug. 2018
[14] H. Mohajeri, **A. Mosenia**, P. Mittal, and N. Feamster, "How ISPs Can Anonymize You: Deployable Anonymity at Network Level," To be submitted to Privacy Enhancing Technologies Symposium (PETS), Aug. 2018
[15] A. Bhagoji, C. Sitawarin, **A. Mosenia**, P. Mittal, and M. Chiang, "Out-of-Distribution Attacks: An Experimental Security Analysis of Secured Convolutional Neural Networks" To be submitted to IEEE Symposium on Security and Privacy, Sep. 2018

Position Papers (Industrial)

[16] B. A. Martin, F. Michaud, D. Banks, **A. Mosenia**, R. Zolfonoon, S. Irwan, S. Schrecker, and J. K. Zao, "OpenFog Security Requirements and Approaches," in Proc. Fog World Congress, 2017 **[Invited paper]**

[17] H. Moustafa, M. Gorlatova, C. Byers, E. Schooler, K. Walcott, J. Acharya, **A. Mosenia**, B. Murthy, C. Vasters, S. Kambhatla, "Autonomous Driving: OpenFog Support Vehicle-to-Cloud", 2017

Selected Professional Activities

Program Committee Member/Reviewer:

- IEEE Trans. Computers
- IEEE Trans. Information Forensics and Security
- IEEE Trans. Dependable and Secure Computing
- IEEE Trans. Biomedical Engineering
- Privacy Enhancing Technologies Symposium (PETS)
- Annual Conference on Information Sciences & Systems
- IEEE Trans. Circuits and Systems II
- IEEE Trans. Network Science and Engineering

Memberships and Affiliations:

- Affiliated with Center of Information Technology and Policy (CITP)
- IEEE Member, Dec. 2013-present
- ACM Member, 2017-present
- Technical Committee Member, OpenFog Consortium, 2017-present
- Technical Member of Security Work Group, OpenFog Consortium, 2017-present
- Technical Member of Testbed Work Group, OpenFog Consortium, 2017-present
- Technical Member, Princeton Research Day Program, 2016
- Technical Committee Member, Fog World Congress, Santa Clara, 2017
- Session Chair, Princeton Research Day Program, 2017
- Panelist and Technical Committee Member, IoT Evolution Expo, Orlando, Florida, 2018

Skills

- Programming: Java, Python, C/C++, Verilog, Matlab
- CAD tools: ISE, Modelsim, HSpice, Design Compiler
- Web technologies: HTML, CSS, PHP, MySQL, Ajax

Invited Presentations

I had several invited presentations in top-tier academic and industrial research institutions across the world:

- Massachusetts Institute of Technology
- International Computer Science Institute (Berkeley)
- IBM Research
- Johns Hopkins University
- New York University
- Texas A&M University
- University of Virginia
- UC Irvine
- University of Georgia
- UC Santa Cruz
- INRIA (Grenoble, France)
- Sharif University of Technology (Tehran, Iran)

Teaching Experience

I served as a teaching assistant for multiple Computer Science/Engineering courses:

- Information Security
- Embedded Computing
- Contemporary Logic Design
- Theory of Languages and Automata
- Computer Architecture
- Electrical Circuits

Additional References

- M. Chiang, John A. Edwardson Dean of the College of Engineering, Purdue University, [chiangm@princeton.edu]
- P. Mittal, Professor of Electrical Engineering, Princeton University [pmittal@princeton.edu]
- N. K. Jha, Professor of Electrical Engineering, Princeton University [jha@princeton.edu]
- A. Raghunathan, Professor of Electrical and Computer Engineering, Purdue University [raghunathan@purdue.edu]
- S. Sur-Kolay, Professor, Advanced Computing and Microelectronics Unit, Indian Statistical Institute [ssk@isical.ac.in]
- M. Mozaffari, Professor of Electrical and Computer Engineering, University of South Florida [mehran2@usf.edu]