Arsalan Mosenia

Last update on August 19, 2018

- https://princeton.edu/~arsalan • arsalan@princeton.edu • +1-(609) 216-2173
- https://www.linkedin.com/in/arsalan-mosenia-5b0a6162/ • INSPIRE Lab, Princeton University

Overview

- 6+ years of research/engineering experience at the intersection of Machine Learning (ML) and Security
- 2+ years of research experience in the security autonomous and Internet-connected vehicles
- Developed several ML-based end-to-end systems for smart cars, security applications, and healthcare
- Currently leading *Autonomous Vehicle Security Team* and *DARTS Project* at *Princeton INSPIRE Lab*
- Examined security vulnerabilities of ML in mission-critical applications, e.g., autonomous driving
- Received several research excellence awards, including the *two most competitive awards* at Princeton that support entrepreneurial ideas (IP Accelerator Award and Innovation Award) for my work on smart/autonomous cars
- Collaborated with the Security Working Group (SWG) at OpenFog [1] to define security standards for Fog industry
- Led 15+ research studies, mentored 20 students, and collaborated with 25+ co-authors across 10 research labs
- 30+ invited presentations in top-tier academic and industrial research institutions across the world

Areas of Expertise

Machine Learning (ML): Applications of ML in Security/Privacy, Adversarial ML, Security Analysis of Learning Methods, and Energy-efficient Learning on Compressed Data

System Security: Security of Internet-connected and Autonomous Vehicles, IoT Security, Edge/Fog Security, Embedded System Security, User Authentication, Security of Smartphones and Wearables, and Healthcare Security

Privacy: Smartphone Privacy, Healthcare Privacy, and Privacy-enhancing Technologies for Autonomous Cars

Education

Princeton University — Princeton, NJ
Ph.D., Electrical Engineering Department (Computer Engineering Division) — *May 2013 – Jan. 2017*
Thesis: Addressing Security and Privacy Challenges in Internet of Things
Key Areas: Secure end-to-end System Design, User Authentication, Hardware/Software Security Analysis, Reverse Engineering, and Applied ML in Security Applications

Princeton University — Princeton, NJ
M.A., Electrical Engineering Department — *Sep. 2012 – May 2013*
Graduate Coursework: Security and Privacy, Machine Learning, Fundamentals of Probability Theory and Random Processes, Information Theory, Surveillance and Countermeasures, Transmission and Compression

Sharif University of Technology — Tehran, Iran
B.Sc., Computer Engineering Department — *Sep. 2008 – May 2012*

Certificates

Specialization in Deep Learning — Coursera, *2018*
Prof. Andrew Ng, Stanford University

Honors and Awards

Intellectual Property Accelerator Award ($100K), Princeton University, 2018 (awarded to my work on smart cars)
Princeton Innovation Award ($200K), Princeton University, 2017 (awarded to my work on the security of smart cars)
Selected Presenter Award, NJ Tech Council, 2017 (awarded to my presentation on user authentication)
French-American Doctoral Exchange Fellowship, 2016 (one of ten selected students in the U.S.)
Project X Award ($100K), Princeton University, 2016 (awarded to my work on continuous authentication)
Spotlight paper, IEEE Trans. Multi-scale Computing Systems, 2015
Multiple Most Popular Papers, 2015-2018 (five of my papers are among the most popular papers of top-tier journals)
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)
Ranked top 1% **(100+ Computer Engineering students)**, Sharif University, Iran, 2008-2012
Ranked top 0.1% **(400,000+ students)**, Nationwide University Entrance Exam, Tehran, Iran 2008

[1] To drive industry and academic leadership in fog computing, OpenFog Consortium was founded by Princeton University and Cisco in 2015. Since then, this consortium has brought together several researchers and designers from the industry (e.g., Intel, Microsoft, Dell, and ARM Holdings) and academia, and it now has over 55 members across North America, Asia, and Europe.

Experience

INSPIRE Lab, Princeton, ML Security Researcher, Host: Prof. P. Mittal — Jan. 2017 – present

- Leading multiple research studies on *adversarial ML* in the *System Security* subgroup
- Developing a secure privacy-aware application development framework for Internet-connected cars
- Exploring privacy concerns associated with the use of Internet-connected cars
- Examining new security threats against computer vision systems utilized in autonomous vehicles

EDGE Lab, Purdue, Postdoc Researcher, Host: Prof. M. Chiang — Jan. 2017 – present

- Active contributor to the Security Working Group (SWG) at OpenFog Consortium
- Developing an end-to-end application development framework, called ProCMotive, which enables secure distributed services for Internet-connected cars (received IP Accelerator Award)
- Developed the first vehicular add-on middleware, called CARWare, for already-in-market vehicles (received Princeton Innovation Award)
- Collaborating with leading technology companies to define security guidelines for Fog Computing
- Examining the security and privacy challenges associated with the use of Internet-connected/Autonomous cars

IoT/ML/Security Lab, Princeton, Ph.D. Candidate, Advisor: Prof. N. K. Jha — May 2013 – Dec. 2016

- Eight first-author papers published in top-tier journals
- Three patents
- Examined applications of ML in IoT security
- Invented a continuous authentication system based on ML and wearable medical devices

Image Processing Lab (IPL), Sharif University, ML Researcher — May 2011 – May 2012

- Led two research studies in the area of computer vision

Leadership and Collaboration

- Led over 15 research studies in the areas of Information Security and User Privacy
- Mentored and co-supervised 20 graduate and undergraduate students
- Collaborated with over 25 co-authors across 10 industrial and academic research labs
- Collaborating with Testbed Working Group at OpenFog Consortium (designing Fog-oriented systems)
- Collaborating with Security Working Group at OpenFog Consortium (defining domain-specific security standards and guidelines for Fog industry)

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)]
[5] Braille-based Keyboard, Intellectual Property Office, Tehran, Iran, 2007

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," 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, "PANEL: Practical 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

Invited Presentations

→ Had over 30 invited presentations in top-tier research institutions across the world, including:

- Massachusetts Institute of Technology
- International Computer Science Institute (Berkeley)
- Johns Hopkins University
- New York University
- Texas A&M University
- Fog World Congress (Keynote Speaker, 2018)
- University of Virginia
- UC Irvine
- UC Santa Cruz
- INRIA (Grenoble, France)
- Sharif University of Technology (Tehran, Iran)
- Domaine universitaire de Grenoble (France)

Teaching Experience

→ 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

Technical Skills

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

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

Technical Committee Member

- OpenFog Consortium, 2017
- Security Working Group, OpenFog Consortium, 2017
- Testbed Working Group, OpenFog Consortium, 2018
- Princeton Research Day (session chair), 2017
- Fog World Congress, 2017
- IoT Evolution Expo, Orlando (panelist), 2017

Writing Proposals: Co-authored several research grant proposals for different governmental agencies, including:

- National Science Foundation (NSF)
- National Institute of Standards and Technology (NIST)
- Office of Naval Research (ONR)