Milad Nasr

Address	Computer Science Building, 140 Governors Drive Amherst, MA, USA 01003	**Phone** **Email** **Homepage**	+1 (413) 406 9557 milad@cs.umass.edu `http://people.cs.umass.edu/~milad`

Education

2018–Present	PhD in Computer Science, University of Massachusetts Amherst	*GPA*: 3.97/4
2015–2018	M.Sc. in Computer Science, University of Massachusetts Amherst	*GPA*: 3.97/4
2011–2015	B.Sc. in Computer Engineering, Isfahan University of Technology	*GPA*: 17.97/20

Research Interests

- **Security and Privacy**
- **Security and Privacy in Machine Learning**
- **Game Theory and Mechanism Design**

Publications

- Xinyu Tang, Saeed Mahloujifar, Liwei Song, Virat Shejwalkar, **Milad Nasr**, Amir Houmansadr, Prateek Mittal *"Mitigating Membership Inference Attacks by Self-Distillation Through a Novel Ensemble Architecture"* 2022 USENIX Security Symposium (**USENIX Security**) (2022).
- **Milad Nasr**, Shuang Song, Abhradeep Guha, Nicolas Papernot and Nicholas Carlini. *"Adversary Instantiation: Lower bounds for differentially private machine learning"* 2021 IEEE Symposium on Security and Privacy. IEEE (**S&P**) (2021).
- **Milad Nasr**, Alireza Bahramali and Amir Houmansadr. *"Blind Adversarial Perturbations for Traffic Analysis"* 2021 USENIX Security Symposium (**USENIX Security**) (2021)
- Xinyu Tang, Saeed Mahloujifar, Liwei Song, Virat Shejwalkar, **Milad Nasr**, Amir Houmansadr, Prateek Mittal *"A Novel Self-Distillation Architecture to Defeat Membership Inference Attacks"* 2021 NeurIPS 2021 Workshop Privacy in Machine Learning (2021)
- Nicholas Carlini, Steve Chien, **Milad Nasr**, Shuang Song, Andreas Terzis, Florian Tramer. *"Membership Inference Attacks From First Principles"* (under submission)
- **Milad Nasr**, Reza Shokri and Amir Houmansadr. *"Improving Deep Learning with Differential Privacy using Gradient Encoding and Denoising"* (under submission)
- Alireza Bahramali, **Milad Nasr** and Amir Houmansadr. *'Robust Adversarial Attacks Against DNN-Based Wireless Communication Systems"* Proceedings of the 28th ACM Conference on Computer and Communications Security. ACM (**CCS**) (2021).
- **Milad Nasr**, Hadi Zolfaghari and Amir Houmansadr. *"MassBrowser: Unblocking the Web for the Masses"* **NDSS** (2020).
- **Milad Nasr** and Michael Tschantz. *"Bidding Strategies with Gender Nondiscrimination: Constraints for Online Ad Auctions"* 2020 ACM Conference on Fairness, Accountability, and Transparency. ACM (**FAT***) (2020).
- **Milad Nasr**, Reza Shokri and Amir Houmansadr. *"Generalizable Deep Learning with Differential Privacy: Using Gradient Compression and De-noising"* 2019 Theory and Practice of Differential Privacy (**TPDP**) (2019).
- **Milad Nasr**, Reza Shokri and Amir Houmansadr. *"Comprehensive Privacy Analysis of Deep Learning: Standalone and Federated Learning under Passive and Active White-box Inference Attacks"* 2019 IEEE Symposium on Security and Privacy. IEEE (**S&P**) (2019).

- **Milad Nasr**, Sadegh Farhang, Amir Houmansadr and Jens Grossklags. *"Enemy At the Gateways: A Game Theoretic Approach to Proxy Distribution."* **NDSS** (2019).
- **Milad Nasr**, Alireza Bahramali and Amir Houmansadr. *"DeepCorr: Strong Flow Correlation Attacks on Tor Using Deep Learning."* Proceedings of the 25th ACM Conference on Computer and Communications Security. ACM (**CCS**) (2018).
- **Milad Nasr**, Reza Shokri and Amir Houmansadr. *"Machine Learning with Membership Privacy using Adversarial Regularization."* Proceedings of the 25th ACM Conference on Computer and Communications Security. ACM (**CCS**) (2018).
- **Milad Nasr**, Anonymous and Amir Houmansadr. *"Poster: Introducing MassBrowser: A Censorship Circumvention System Run by the Masses"* Poster at IEEE Security and Privacy (**SP**) (2018).
- **Milad Nasr**, Hadi Zolfaghari and Amir Houmansadr. *"The Waterfall of Liberty:Decoy Routing Circumvention that Resists Routing Attacks."* Proceedings of the 24th ACM Conference on Computer and Communications Security. ACM (**CCS**) (2017).
- **Milad Nasr**, Amir Houmansadr and Arya Mazumdar. *"Compressive Traffic Analysis:A New Paradigm for Scalable Traffic Analysis."* Proceedings of the 24th ACM Conference on Computer and Communications Security. ACM (**CCS**) (2017).
- **Milad Nasr**, and Amir Houmansadr. *"Game of Decoys: Towards Optimal Decoy Routing Circumvention Through Game Theory."* Proceedings of the 23rd ACM Conference on Computer and Communications Security. ACM (**CCS**) (2016).
- Stanford, H. C. I. *"Daemo: a Self-Governed Crowdsourcing Marketplace"* . Adjunct Proceedings of the 28th Annual **ACM Symposium on User Interface Software & Technology**(2015).
- S.Farhang, M. H.Manshaei, **M. N.Esfahani**, and Q.Zhu, *"A Dynamic Bayesian Security Game Framework for Strategic Defense Mechanism Design",* in **Decision and Game Theory for Security** (pp. 319-328). Springer International Publishing (2014).

Research Experience

- Research intern at Google Research, *Fall 2021*
- Research intern at Facebook, *Summer 2021*
- Research intern at Google Brain, *Summer 2020*
- Researcher at University of Massachusetts Amherst Security and Privacy Group (SPIN), *Fall 2015-Present*
- Research intern at International Computer Science Institute (ICSI), *Summer 2018*
- Researcher at Stanford Crowd Research Collective Group, *Spring 2015*
- Researcher at Isfahan University of Technology Game Theory and Mechanism Design Laboratory (GTMD), *Fall 2013-Spring 2015*

Academic Services

- Invited Talks:
  - Oracle: *Adversary Instantiation: Lower bounds for differentially private machine learning* (Summer 2021)
  - Facebook: *Adversary Instantiation: Lower bounds for differentially private machine learning* (Summer 2021)
  - University of Toronto: *Adversary Instantiation: Lower bounds for differentially private machine learning* (Spring 2021)
  - University of Carnegie Mellon University: *Membership Leakage Through Deep Learning Models* (Spring 2020)

  - University of Boston: *Membership Leakage Through Deep Learning Models* (Fall 2019)
  - University of Connecticut: *Advanced Traffic Analysis* (Fall 2018)
- Reviewer:
  - IEEE Transactions on Information Forensics and Security 2020
  - Privacy Enhancing Technologies Symposium (PETS) 2020
  - Transactions on Dependable and Secure Computing 2020
  - IEEE Transactions on Signal and Information Processing over Networks 2019
  - IEEE Transactions on Information Forensics and Security 2019
  - Student PC IEEE Security and Privacy (S&P) 2019
  - Privacy Enhancing Technologies Symposium (PETS) 2019
  - IEEE Communications Letters 2018
  - Privacy Enhancing Technologies Symposium (PETS) 2018
- PC:
  - Privacy Enhancing Technologies Symposium (PETS) 2022
  - The ACM Conference on Computer and Communications Security (CCS) 2021
  - Privacy Enhancing Technologies Symposium (PETS) 2021

Awards and Honors

- Google PhD Fellowship in Security and Privacy, 2019
- Outstanding Graduate Student Award for Master Synthesis Project (equivalent of master thesis), University of Massachusetts Amherst, 2017
- Ranked 8th in "Master of Computer Engineering (AI)" nationwide entrance exam, Iran, 2015
- Top 3 among 60 students in computer engineering, Isfahan University of Technology, 2015
- Granted merit-based admission to masters program in AI, Network and Software Engineering at ECE department of Isfahan University of Technology, 2014
- Certificate from NIIT in "Object Oriented Application Development" with outstanding score, 2008
- Winner of National Organization for Development of Exceptional Talents (NODET) software competition, 2007
- Winner of software festival in middle-school National Organization for Development of Exceptional Talents (NODET) competition, 2005–2006

Projects

- **MassBrowser** Volunteer based censorship circumvention system (available at `https://massbrowser.cs.umass.edu/`), *2017-Present*
- **SIDS** Anomaly detection system using statistical features of network traffic, Isfahan University of Technology, *2014*
- **IUT ECE Computing Cluster** High performance cluster for parallel computing, Department of Electrical and Computer Engineering at Isfahan University of Technology, *2014*
- **IUT Domain** Campus wide central windows domain using Samba, LDAP and DNS with more than 5000 PCs, more than 20000 users with load balancing and failover, Isfahan University of Technology, *2012*
- **IUT boinc** Campus volunteer computing system with more than 300 PC and 500GFlops computing power, Isfahan University of Technology, *2012*
- **Robocup Junior Soccer** Programmer and Electrical designer in Junior Soccer Robotic team, Shahid Ejei high school, *2008-2010*

Professional Experience

2011– 2015 Information Technology Center-Isfahan University of Technology, *Isfahan, Iran*
Researcher and Network Administrator

- IUTBackup: Designing and deployment of a distributed storage
- IUTCloud: Deploying IaaS with OpenStack
- Kharazmi System: Designing a cloud based homepage for IUT faculty members

2013– 2015 Omid Programming Company, *Isfahan, Iran*
CEO/Project Manager

- Mobile Programming (iOS/Android)
- Backend Programming (Python)

Software Engineering Skills

- **Programming Languages**
  Python, Java, Nodejs, GO, C, C++, C#

- **Deep Learing Frameworks**
  Tensorflow, PyTorch

- **Network Administration**
  FreeBSD, Cisco iOS, Windows, UNIX, Clustering, Virtualization

Teaching Experience

- University of Massachusetts Amherst
  - Teaching Assistant :
    Introduction to Computer and Network Security (Fall 2017)
- Shahid Ejei High School
  - Teacher:
    Game Theory (Summer 2014), C# Programming (Summer 2012–2014), AVR Programming (Summer 2012), C++ Programming (Summer 2011), Information Security (Summer 2010)
- Isfahan University of Technology
  - Teaching Assistant:
    Parallel Processors (Spring 2012–2015), Computer Programming (Fall 2013)
  - Volunteer Teaching:
    MPI Programming (Summer 2013), Cisco Switches (Summer 2012), Linux (Summer 2012)

Language Skills

- **English**- Fluent
- **Persian**- Native

References

Available upon request.