

Eugene Bagdasaryan

eugene@cs.cornell.edu

SUMMARY:

PhD candidate at Cornell Tech aiming to build ethical, safe, and private machine learning.

EDUCATION:

Cornell Tech, Cornell University

Aug 2016 – present

Pursuing PhD in Computer Science. Focused on security and privacy in ML: federated learning, differential privacy, backdoors. Advised by Professors Vitaly Shmatikov and Deborah Estrin.

Dec 2019 – Master's degree in Computer Science

Bauman Moscow State Technical University, Russia

Sep 2009 – Jun 2016

June 2016 – Engineer's degree in Computer Science, diploma with honors. Focus: AI and Systems, GPA: 3.9/4.0

June 2013 – Bachelor's degree in Computer Science, diploma with honors. GPA: 4.0/4.0.

AWARDS:

- Apple AI/ML Fellowship'21.
- Digital Life Initiative Fellowship'19.
- Bloomberg Fellowship'17.
- Vladimir Potanin Scholarship '11, '12 and '13.
- Russian Government Scholarship'12.
- Bauman Academic Excellence Fellowship'11, '12.

WORK EXPERIENCE:

Cisco Systems Innovation Center, Moscow, Russia

Sep 2014 – Jul 2016

Software Engineer 2 at the Cloud Group, developing and testing large scale OpenStack project.

INTERNSHIPS:

Apple, Cupertino, CA

May 2021 – Aug 2021

Conducted research on Federated Learning and Language Models.

Google Research, NYC

May 2020 – Aug 2020

Did research on Local Differential Privacy and Secure Aggregation for Federated Analytics.

Amazon, Seattle, WA

May 2018 – Aug 2018

Worked on a novel multi-service recommendations engine for Alexa.

Cisco Systems, Boston, MA

Aug 2013 – Jul 2014

Developed front-end and back-end for the SocialMiner data analytics web application.

Deloitte Touché Tohmatsu Limited, Moscow, Russia

Dec 2012 – Apr 2013

Performed data analytics tasks for the audit department.

PUBLICATIONS:

- **BE**, Shmatikov V: “Spinning Language Models for Propaganda-As-A-Service”, Preprint 2021.
Media Coverage: VentureBeat.
- **BE**, Kairouz P, Mellem S, Gascón A, Bonawitz K, Estrin D, Gruteser M.: “Towards Sparse Federated Analytics: Location Heatmaps under Distributed Differential Privacy with Secure Aggregation.” Preprint 2021.
- **BE**, Shmatikov V.: “Blind Backdoors in Deep Learning Models”, in USENIX Security’21. **Media Coverage:** Cornell Chronicle, ZDNet.
- **BE**, Veit A, Hua Y, Estrin D, Shmatikov V. “How to Backdoor Federated Learning”, in AISTATS’20.
- Katevas K, **BE**, Waterman J, Safadiéh MM, Birrell E, Haddadi H, Estrin D. “Policy-based federated learning”. Preprint 2020.
- Yu T, **BE**, Shmatikov V: “Salvaging Federated Learning using Local Adaptation”, Preprint 2020.
- **BE**, Shmatikov V: “Differential Privacy Has Disparate Impact on Model Accuracy”, in NeurIPS’19.
- **BE**, Berenstein G, Waterman J, Birrell E, Foster N, Schneider F, Estrin D: “Ancile: Enhancing Privacy for Ubiquitous Computing with Use-Based Privacy”, in WPES’19. **Media Coverage:** Cornell Chronicle, TechXplore.
- Yang L, **BE**, Gruenstein J, Hsieh C.-K, Estrin D: “OpenRec: A Modular Framework for Extensible and Adaptable Recommendation Algorithms”, in WSDM’18.

INVITED TALKS:

- “Blind Backdoors in Deep Learning Models”, UCL, December 2021.
- “Blind Backdoors in Deep Learning Models”, University of Cambridge, November 2021.
- “Federated Learning with Local Adaptation: Addressing Security and Privacy Tradeoffs”, Telefonica Research, September 2021.
- “Privacy Preserving Techniques in Machine Learning”, Microsoft Research Talks, February 2021.

- “Salvaging Federated Learning with Local Adaptation”, Google Federated Learning Talks, June 2020.
- “Evaluating Privacy Preserving Techniques in Machine Learning”, Digital Life Initiative Seminar Series, Feb 2020.
- “Contextual Recommendation Sharing”, 2nd Symposium on Contextual Integrity, July 2019.

SERVICE:

- Reviewer: NeurIPS’21, ICLR’22, FL@ACL’22.