Eugene Bagdasaryan
1 East Loop Rd 22 A, New York, NY, 10044
eugene@cs.cornell.edu

SUMMARY:

5th year CS PhD Candidate studying privacy and security for machine learning systems.

EDUCATION:

CornellTech, Cornell University *Aug 2016 – present*

PhD candidate in Computer Science department. Focused on security and privacy in ML, Federated Learning, Differential Privacy, Recommender Systems. Advised by Professors Deborah Estrin and Vitaly Shmatikov.

Bauman Moscow State Technical University, Russia *September 2009 – 2016*

June 2016 – Master'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

WORK EXPERIENCE:

CornellTech, Cornell University *September 2016 – present*

Research Assistant (small data lab), Teaching Assistant (Systems Spring'17, Fall'18, Spring'20, Databases Fall'16)

Cisco Systems *September 2014 – July 2016*

QA Software Engineer at Cloud and Virtualization Group, focused on OpenStack Networking

INTERNSHIPS:

Google Research, NYC *May 2020 – Aug 2020*

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

Amazon, Seattle, WA *May 2018 – Aug 2018*

Worked on novel multi-service recommendations engine for Alexa.

Cisco Systems, Boston, MA *August 2013 – July 2014*

Software Engineering Intern worked on SocialMiner web-app.

Deloitte Touché Tohmatsu Limited, Moscow, Russia *December 2012 – April 2013*

Worked on data analysis for audit department.

PAPERS:

- **E.B.**, V. Shmatikov: "Blind Backdoors in Deep Learning Models" [in submission, arXiv]
- **E.B.**, A. Veit, Y. Hua, D. Estrin, V. Shmatikov: "How to Backdoor Federated Learning" [AISTATS'20]
- T. Yu, **E.B.**, V. Shmatikov: "Salvaging Federated Learning using Local Adaptation" [arXiv]
- **E.B.**, V. Shmatikov: "Differential Privacy Has Disparate Impact on Model Accuracy" [NeurIPS'19]
- **E.B.**, G. Berlstein, J. Waterman, E. Birrell, N. Foster, F. Schneider, D. Estrin: "Ancile: Enhancing Privacy for Ubiquitous Computing with Use-Based Privacy" [WPES'19]
- L.Yang, **E.B.**, J. Gruenstein, C.-K. Hsieh, D. Estrin: "OpenRec: A Modular Framework for Extensible and Adaptable Recommendation Algorithms" [WSDM '18]

AWARDS:

- 2019-2020 Digital Life Initiative Fellowship
- Bloomberg Data Immersion Day 2017 Fellowship
- 3x winner of the Vladimir Potanin Scholarship, in '11, '12 and '13
- Russian Government Scholarship for Science Research, Academic Council Faculty Fellowship