EUGENE BAGDASARYAN

eugene@cs.cornell.edu

SUMMARY:

I am a PhD candidate at Cornell CS aiming to build ethical, safe, and private machine learning.

EDUCATION:

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 Deborah Estrin and Vitaly Shmatikov.

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, with honors. GPA: 3.9/4.0

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

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:

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:

- **B.** and Shmatikov: "*Blind Backdoors in Deep Learning Models*", in USENIX Security'21.
- **B.**, Veit, Hua, Estrin, Shmatikov: "*How to Backdoor Federated Learning*", in AISTATS'20.
- Yu, **B.**, Shmatikov: "*Salvaging Federated Learning using Local Adaptation*", ArXiv'20.

- **B.** and Shmatikov: "*Differential Privacy Has Disparate Impact on Model Accuracy*", in NeurIPS'19.
- **B.**, Berlstein, Waterman, Birrell, Foster, Schneider, Estrin: "*Ancile: Enhancing Privacy for Ubiquitous Computing with Use-Based Privacy*", in WPES'19. **Media Coverage**: Cornell Chronicle, TechXplore.
- Yang, **B.**, Gruenstein, Hsieh, Estrin: "*OpenRec: A Modular Framework for Extensible and Adaptable Recommendation Algorithms*", in WSDM'18.

AWARDS:

- 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.

INVITED TALKS:

- "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, DPML'21, MAISP'21.
- Cornell Tech PhD Student body leadership team, '18,'19.