# Eugene Bagdasaryan

eugene@cs.cornell.edu

SUMMARY:

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

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, 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:

**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:

- **E.B.**, V. Shmatikov: "Blind Backdoors in Deep Learning Models", in submission.
- **E.B.**, A. Veit, Y. Hua, D. Estrin, V. Shmatikov: "How to Backdoor Federated Learning", in AISTATS'20.

- T. Yu, **E.B.**, V. Shmatikov: “Salvaging Federated Learning using Local Adaptation”, in submission.
- **E.B.**, V. Shmatikov: “Differential Privacy Has Disparate Impact on Model Accuracy”, in 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”, in WPES’19. **Media Coverage**: Cornell Chronicle, TechXplore.
- L.Yang, **E.B.**, J. Gruenstein, C.-K. Hsieh, D. 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:

- “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.