EUGENE BAGDASARYAN

eugene@cs.cornell.edu

SUMMARY:

I am a CS PhD candidate at Cornell 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, defenses against backdoor attacks. Advised by Professors Deborah Estrin and Vitaly Shmatikov. Minor in Business Administration.

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 Cloud Group, contributor to the OpenStack Networking 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 science tasks to assist in client audit.

PUBLICATIONS:

- Bagdasaryan, E. and Shmatikov, V., "Blind Backdoors in Deep Learning Models", in USENIX Security'21.
- Bagdasaryan, E., Veit, A., Hua, Y., Estrin, D. and Shmatikov, V., "*How to Backdoor Federated Learning*", in AISTATS'20.

- Yu, T., Bagdasaryan, E. and Shmatikov, V., "*Salvaging Federated Learning using Local Adaptation*", technical report.
- Bagdasaryan, E. and Shmatikov, V., "*Differential Privacy Has Disparate Impact on Model Accuracy*", in NeurIPS'19.
- Katevas, K., Bagdasaryan, E., Waterman, J., Safadieh, M.M., Birrell, E., Haddadi, H. and Estrin, D., "*Policy-Based Federated Learning*", technical report.
- Bagdasaryan, E., Berlstein, G., Waterman, J., Birrell, E., Foster, N., Schneider, F.B. and Estrin, D., "*Ancile: Enhancing Privacy for Ubiquitous Computing with Use-Based Privacy*", in WPES'19. **Media Coverage**: Cornell Chronicle, TechXplore.
- Shen, Z., Sun, Z., Sela, G.E., Bagdasaryan, E., Delimitrou, C., Van Renesse, R. and Weatherspoon, H., "*X-containers: Breaking down barriers to improve performance and isolation of cloud-native containers."* In *ASPLOS*'19.
- Yang, L., Bagdasaryan, E., Gruenstein, J., Hsieh C.K. and Estrin D., "*OpenRec: A Modular Framework for Extensible and Adaptable Recommendation Algorithms*", in WSDM'18.
- Behrens, J., Birman, K., Jha, S., Milano, M., Tremel, E., Bagdasaryan, E., Gkountouvas, T., Song, W. and Van Renesse, R., "*Derecho: Group communication at the speed of light*", technical report.

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.
- Tutorial on "*Modularizing deep neural network-inspired recommendation algorithms*", WSDM'19

SERVICE:

- Reviewer: NeurIPS’21, DPML’21, MAISP’21.
- Cornell Tech PhD Student body leadership team, ’18,’19.