CONGZHENG SONG

Curriculum Vitae

Contact

Email: cs2296@cornell.edu
Address: 2 W Loop Rd, New York, NY, 10044
Homepage: `https://www.cs.cornell.edu/~csong/`

Education

Cornell University, Ithaca, NY 2016 – Present
Ph.D. student in Computer Science
Research Interests: Security and Privacy in Machine Learning

Emory University, Atlanta, GA 2012 – 2016
B.S. in Computer Science with Summa Cum Laude
Thesis: *Using Deep Recurrent Neural Networks to Estimate Influenza Prevalence from Mobile Phone Records*

Publications

* indicates equal contribution

Peer-reviewed Journal & Conference

1. **Exploiting Unintended Feature Leakage in Collaborative Learning**
   Luca Melis*, **Congzheng Song***, Emiliano De Cristofaro, Vitaly Shmatikov
   To appear in *40th IEEE Symposium on Security and Privacy* (S&P), San Francisco, California, 2019
2. **Predicting Clinical Outcomes from Large Scale Cancer Genomic Profiles with Deep Survival Models**
   Safoora Yousefi, Fatemeh Amrollahi, Mohamed Amgad, Coco Dong, Joshua E. Lewis, **Congzheng Song**, David A. Gutman, Sameer H. Halani, Jose Enrique Velazquez Vega, Daniel J. Brat, Lee A.D. Cooper
   In *Scientific Reports 7* (Nature), 2017
3. **Machine Learning Models that Remember Too Much**
   Congzheng Song, Thomas Risternpart, Vitaly Shmatikov
   In *the ACM Conference on Computer and Communications Security* (CCS), Dallas, Texas, 2017
4. **Membership Inference Attacks against Machine Learning Models**
   Reza Shokri, Marco Stronati, **Congzheng Song**, Vitaly Shmatikov
   In *38th IEEE Symposium on Security and Privacy* (S&P), San Jose, California, 2017

Workshop & Poster

1. **Kernel Distillation for Fast Gaussian Processes Prediction**
   Congzheng Song*, Yiming Sun*
   To appear in *NIPS Workshop on All of Bayesian Nonparametrics* (BNP@NIPS), Montreal, Canada, 2018
2. **What Are Machine Learning Models Hiding?**
   Vitaly Shmatikov, **Congzheng Song**
   In *11th Workshop on Hot Topics in Privacy Enhancing Technologies* (HotPETs), Barcelona, Spain, 2018
3. **Learning Genomic Representations to Predict Clinical Outcomes in Cancer**
   Safoora Yousefi, **Congzheng Song**, Nelson Nauata, Lee Cooper
   In *International Conference on Learning Representation Workshop* (ICLR), San Juan, Puerto Rico, 2016

Research Experience

Graduate Research Assistant 2016 – Present
Department of Computer Science, Cornell University Adviser: Prof. Vitaly Shmatikov
∞ Exploring privacy leakage in machine learning models.

Undergraduate Research Assistant 2015 – 2016
Department of Math & CS, Emory University Adviser: Prof. Ymir Vigfusson
∞ Extracted a set of metrics to describe human behavior from mobile phone records.
∞ Developed a deep learning model for individual sickness prediction given behavioral features.

Undergraduate Research Assistant 2015 – 2016
Department of Bioinformatics, Emory University Adviser: Prof. Lee Cooper
∞ Developed a neural network combining with Cox regression for survival analysis.
∞ Applied covolutional neural network in cancer cell image classification.

Undergraduate Research Intern Summer 2015
Department of Computer Science, UC Irvine Adviser: Prof. Sharad Mehrotra
∞ Developed a web framework for collecting, querying and visualizing sensor data.
∞ Involved in implementing backend server modules to handle user's request for processing sensors' data on multiple platforms.

Teaching Experience

Graduate Teaching Assistant Fall 2016
CS 3410: Computer System Organization and Programming Instructor: Prof. Anne Bracy

Undergraduate Lab Teaching Assistant Fall 2013
Chem 141: General Chemistry I Instructor: Prof. Karl Hagen

Awards

∞ Trevor Evans Award 2016
∞ Deborah Jackson Award 2015
∞ Dean's List 2012 – 2016

Skills

Programming and Scripting Languages: Python, Java, C, JavaScript, HTML & CSS, LaTeX

Software and Tools: Tensorflow, Theano, Matlab, R studio, Node.js, MongoDB, PostgreSQL