Yunhui Long

907 W. Stoughton Street Apt 313, Urbana, IL 61801 +1(217)607-6237 | ylong4@illinois.edu

Education

- **PhD | University of Illinois at Urbana-Champaign** Urbana, IL, USA
  Computer Science; GPA:3.93/4.0 *Aug. 2014 – May 2019(expected)*
  - Key Courses: Data Mining, Machine Learning, Computer Security, Operating System, Distributed System, Cryptocurrency
- **BSc | Beijing University of Posts and Telecommunications** Beijing, China
  Telecommunications Engineering with Management; GPA:3.8/4.0 *Sep. 2010 – June 2014*
  - Key Courses: Data Structure, Database, Software Engineering, Digital Signal Processing, Image and Video Processing, 3D Graphics Programming Tools, Multimedia System, Network Application, Wireless Network
  - Rank: 2/363
- **BSc | Queen Mary University of London** London, UK
  Joint Program with Beijing University of Posts and Telecommunications

Experience

- **University of Illinois at Urbana-Champaign** Urbana, IL, USA
  Research Assistant *Aug. 2014 – Dec. 2015, Aug. 2016 – Present*
  - **Advisor:** Prof. Carl Gunter
  - **Research Areas:** Privacy, Machine Learning, Security, and Blockchain
- **Chinese Academy of Science** Beijing, China
  Research Intern *May 2017 – Aug. 2017*
  - **Advisors:** Prof. Xiaofeng Wang, Prof. Kai Chen
  - Analyzed privacy risks of commonly used machine learning models including neural networks
  - Designed adversarial machine learning attacks on speech recognition systems
- **Palo Alto Research Center, a Xerox Company** Palo Alto, CA, USA
  Research Intern (Interactions and Analytics Lab) *Jun. 2016 – Aug. 2016*
  - **Mentors:** Frank Torres, Vanishree Rao
  - Integrated privacy protection layer into automatic machine learning tools
  - Analyzed the trade off between privacy and utility for machine learning models
  - Designed cryptographic tools for privacy-preserving feature selection
- **University of Illinois at Urbana-Champaign** Urbana, IL, USA
  Teaching Assistant *Jan. 2016 – May 2016*
  - **Course:** CS463 Computer Security II
  - Designed lectures on **Machine Learning in Security**, and **Adversarial Machine Learning**
  - Designed machine problem on **De-Anonymization of Bitcoin Network**

Awards

- **Chirag Foundation Graduate Fellowship in Computer Science**
  Chirag Foundation & University of Illinois at Urbana-Champaign *2014*
  - Awarded to one student in UIUC each year
- **National Scholarship**
  Ministry of Education of China *2011, 2012, 2013*
  - Awarded to top 4 out of 363 each year
- **Meritorious Winner in Mathemmatical Contest in Modeling**
  the Consortium for Mathematics and its Applications *2013*
  - Awarded to top 10 to 15% of teams

Ongoing Research

- **Analyzing Correlations between Privacy Risks and Model Generalizations**
  Chinese Academy of Science
  - Identified the correlations and differences between privacy risks and model generalizations
  - Studied each training record's influence on the machine learning model's predictions on different queries
  - Designed new membership inference attacks that work on models with good generalizations
- **Calculating Membership Privacy**
  University of Illinois at Urbana-Champaign
  - Proposed an empirical metric to measure privacy leakage of black-box machine learning models
  - Proposed new membership inference attacks on black-box machine learning models
  - Experimentally measured the privacy risk of different machine learning models
  - Validated the empirical metric's strong correlations with risks of real attacks
- **Self-Tallying Multi-party Secure Aggregation**
  University of Illinois at Urbana-Champaign
  - Proposed a protocol for validating and aggregating encrypted inputs from different users
  - Studied how the protocol can be used for machine learning in private and distributed settings
  - Implemented the protocol using Elliptic-Curve Elgamal and evaluated its efficiency

Publications

1. Vanishree Rao and **Yunhui Long**. Differential privacy vs. end-to-end encryption—it's privacy vs. privacy! http://www.infosecisland.com/blogview/24830-Differential-Privacy-vs-End-to-end-Encryption--Its-Privacy-vs-Privacy.html, 2016
2. **Yunhui Long**, Vincent Bindschaedler, Shubhra Kanti Karmaker Santu, Carl Gunter, and Chengxiang Zhai. Evaluations on privacy risks under sensitive attribute inference attacks. Poster in 2015 USENIX Summit on Information Technologies for Health, 2015
3. Mingyang Lv, **Yunhui Long**, Qianyun Zhang, Xinyu Sheng, Li Xu, Hang Guo, Wenbo Zhang, and Xiaoguang Zhang. A fast polarimeter calibration method using vector projection algorithm. In *Advanced Infocomm Technology (ICAIT), 2013 6th International Conference on*, pages 15–16. IEEE, 2013

Skills

Languages and Tools: Java, Python, Lua, MATLAB, SQL, Torch, TensorFlow, Serpent

Research Interests: Privacy, Machine Learning, Security, and Blockchain