Ningfei Wang

Address: 609 Saucon View Drive, Bethlehem, PA, 18015
Email: ningfei.wang@uci.edu | Tel: 1-610-653-3849 | Website: http://me.ningfei.org

EDUCATION

- **University of California, Irvine** — California, USA
  Ph.D. in Computer Science – Advisor: Qi Alfred Chen — *Sep 2019 – Present*
- **Lehigh University** — Pennsylvania, USA
  M.S. in Computer Science; Overall GPA: 3.94/4.00 — *Aug 2017 – May 2019*
- **Beijing University of Posts and Telecommunications (BUPT)** — Beijing, China
  B.E. in Information Engineering; Overall GPA: 84.7/100.0; Major GPA: 88.7/100.0 — *Aug 2013 – Jun 2017*

RESEARCH EXPERIENCE

- **Interpretable Deep Learning under Fire** — Lehigh University, USA
  Research Assistant, ALPS lab (Prof. Ting Wang) — *Sep 2018 - Jun 2019*
  - **Description**: Provided a broad class of attacks that generate adversarial inputs, which not only mislead target DNN models but also deceive their coupled interpretation models(saliency map models). The paper was accepted by USENIX Security 2020.
  - **Contribution**: Converted Caffe model and TensorFlow model into PyTorch and trained DNN (Resnet and Densenet) on ImageNet. Generated adversarial examples and their saliency map. Evaluated the successful rate of the attacks and distances of saliency map between adversarial examples and benign. Deployed a potential countermeasure – Adversarial Training on RTS.
- **Code De-anonymization** — Lehigh University, USA
  Research Assistant, ALPS lab (Prof. Ting Wang) — *Mar 2018 - Jul 2018*
  - **Description**: Developed SUNDAE, a novel code de-anonymization framework which integrates both static and dynamic stylometry analysis. The paper was accepted by the 11th ACM Workshop on Artificial Intelligence and Security and we won the **best paper award**.
  - **Contribution**: Extracted static and dynamic features(ignored by previous works) of Python source codes. Designed a stylometry matcher based on Siamese Network, which contributes to predicting the similarity of source codes from different programmers. Our approach outperformed the state-of-art methods by a margin of 45.65%.
  - **Github Repository**: https://github.com/ningfeiwang/Code_De-anonymization
- **UniGL: Preventing WebGL-based Browser Fingerprinting** — Lehigh University, USA
  Research Assistant, SEC lab (Prof. Yinzhi Cao) — *Oct 2017 - Jul 2018*
  - **Description**: Developed UNIGL to rewrite OpenGL shading language (GLSL) programs and uniformized WebGL rendering procedure based on different browsers. Defended against browsers fingerprinting from rendering different WebGL task. The paper was accepted by USENIX Security 2019.
  - **Contribution**: Converted the vertex shader to a JavaScript program and execute it. Redefined floating-point operations in fragment shader via integer simulation. Developed a website which connected with back-end MySQL database to collect rendering results and machines hardware features (e.g., DataURL, Agent).
  - **Github Repository**: https://github.com/ningfeiwang/dwebgl.github.io
- **Browser Fingerprint** — Lehigh University, USA
  Developer, SEC lab (Prof. Yinzhi Cao) — *Oct 2017 - Dec 2017*
  - **Description**: Made a large-scale browser fingerprinting analysis (including significant state-of-art features) influenced by different software installed the systems.
  - **Contribution**: Deployed features-collection URL to obtain features and send them to the back-end MySQL database. Deployed "AutoTest" which was to install software automatically and visited the URL. Analyzed the robustness and uniqueness of the features.
  - **Github Repository**: https://github.com/ningfeiwang/install_exe_auto
- **Botnet Detection** — Lehigh University, USA
  Research Assistant, WiNS lab (Prof. Mooi Choo Chuah) — *Sep 2017 - Dec 2017*
  - **Description**: Designed GUI, which was applied to the SEEDS 2017 Industrial Engagement Meeting in Lehigh University, and built simulations for botnet detection.

- **Contribution**: Designed GUI to present network structure and virus-infected network nodes by Python. Conducted three types of network simulation: Query-Response-Acknowledge, Query(Command)-Acknowledge, Query(Command) only, by Omnet++.

- **The Implement of Managing Heterogeneous Cloud with OpenStack** BUPT, China
  Developer and Author, Advisor: Prof. Yang Peng *Sep 2016 - May 2017*
  - **Description**: Managed OpenStack cloud and VMware cloud by OpenStack and completed the graduation paper.
  - **Contribution**: Deployed OpenStack cloud and VMware cloud environments. Utilized Nova Module (computing module in OpenStack) to control OpenStack cloud and VMware Driver. Displayed the details of the two clouds management (e.g., memory usage, network) in web pages. Designed algorithms to solve cloud environments resource scheduling.

- **Inellient Omnidirectional Imaging System (VR)** Tsinghua University, China
  Developer, Advisor: Prof. Xiangyang Ji *Feb 2016 - Aug 2016*
  - **Description**: Deployed omnidirectional imaging system based on OpenCV whose real-time effect is comparable to the Singularity Vision.
  - **Contribution**: Collected videos with six GoPro cameras, divided them into frames, compiled and used Hugin to accomplish image stitching. Extracted features of images by Sift and Surf algorithm with OpenCV. Detected overlapping and generated mask by features. Optimized our system by refining the source code and parallelization.

INTERNSHIP

- **Machine Learning Intern** Cheetah Mobile, China
  Machine Learning Department *Mar 2017 - Jun 2017*
  - **Work Content**: Learned the algorithms of Deep Learning (e.g., Neural Networks, Convolutional Neural Network and Recurrent Neural Networks). Accomplish RNN and LSTM algorithms by C++. Optimized the Cheetahs English text input method by re-constructing the *Trie*.
  - **Achievement**: Grasped many machine learning algorithms(e.g., CNN, RNN, GRU, and LSTM). Trained data through GPU and enhanced my operation of Linux and my knowledge of input methods.

PUBLICATION

1) *Interpretable Deep Learning under Fire*
   Xiangyang Zhang, **Ningfei Wang**, Hua Shen, Shouling Ji, Xiapu Luo, Ting Wang
   The 29th USENIX Security Symposium (Spring Quarter Submission)

2) *Rendered Private: Making GLSL Execution Uniform to Prevent WebGL-based Browser Fingerprinting*
   Shujiang Wu, Song Li, Yinzhi Cao, **Ningfei Wang**
   The 28th USENIX Security Symposium (Fall Quarter Submission, 25/254 = 9.8%)

3) *Integration of Static and Dynamic Code Stylometry Analysis for Programmer De-anonymization*
   Ningfei Wang, Shouling Ji, Ting Wang
   The 11th ACM Workshop on Artificial Intelligence and Security (AISec 2018) **Best Paper Award**

HONORS & AWARDS

- **Excellence Fellowship (Top 5),** UCI CS Department Excellence Fellowship for AY 19/20 2019-2020
- **Best Paper Award,** The 11th ACM Workshop on Artificial Intelligence and Security (AISec 2018) 2018
- **Third Prize,** Scholarship in BUPT for Three Years 2014-2016
- **Excellent Vice-Minister Honor,** Sports Department of Students Union, BUPT 2016
- **Second Place,** the Game of Go on The BUPT Mind Sports Games 2016
- **Second Prize in Beijing Region,** National College Students Innovative Projects 2016
- **Honorable Mention,** Interdisciplinary Contest in Modeling 2016
- **Second Prize,** Contemporary Undergraduate Mathematical Contest in Modeling 2015

SKILLS & HOBBIES

- **Programming Language:** Python, C++, C, Javascript, Matlab
- **Framework:** MySQL, Keras, Scikit-Learn, OpenCV, TensorFlow, PyTorch, TBB, OpenMP
- **Hobbies:** Game of GO, Accordion