JIAMENG PU

jmpu@vt.edu · (540) 418-5306 · https://jmpu.github.io/

EDUCATION

Ph.D. in Computer Science (Expected May 2022) Aug. 2017 – Present

Advisor: Dr. Bimal Viswanath

Virginia Polytechnic Institute and State University, Blacksburg, VA
Research Interests: Data-driven security, machine learning

B. Eng in Computer Science Aug. 2013 – May. 2017

Wuhan University, Wuhan, China

HONORS AND AWARDS

Visa Research Scholarship, awarded by IEEE S&P'20 in San Francisco, CA. May. 2020
Student Travel Grant, awarded by NDSS'19 in San Diego, CA. Feb. 2019
National Endeavor Scholarships, awarded by Chinese Ministry of Education. 2014, 2015

EMPLOYMENT

Graduate Research Assistant at Virginia Tech Nov. 2018 – Present

Advisor: Dr. Bimal Viswanath

- Developing defenses against AI-generated media content, e.g., GAN-synthetic images, Deepfake videos.
- Investigating misdiagnosis threats brought by AI-generated medical images in healthcare system.
- Investigating defense strategies against trojan attacks on deep text models

Data Scientist Intern at IBM China Development Labs Aug. 2016 – Nov. 2016

Advisor: Xinyu Wu (Senior Researcher)

- Simulated the progress of network propagation using deep learning models.
- Made predictions for business scenarios based on survival analysis and machine learning algorithms.

Undergraduate Research Assistant at Wuhan University Aug. 2015 – Aug. 2016

Advisor: Dr. Bo Du, Dr. Lefei Zhang

- Proposed a new robust multiview clustering algorithm based on matrix approximation.

PUBLICATIONS

- "NoiseScope: Spotting Deepfake Images in a Blind Setting", **Jiameng Pu**, Neal Mangaokar, Bolun Wang, Chandan Reddy, Bimal Viswanath. ***To appear, ACSAC(The Annual Computer Security Applications Conference) 2020, Online, December 2020***.
- "Jekyll: Attacking Medical Image Diagnostics Using Neural Translation", Neal Mangaokar, **Jiameng Pu**, Parantapa Bhattacharyam, Chandan Reddy, Bimal Viswanath. ***IEEE EuroS&P 2020, Online, September 2020***.
- "Throwing Darts in the Dark? Detecting Bots with Limited Data using Neural Data Augmentation", Steve T.K. Jan, Qingying Hao, Tianrui Hu, **Jiameng Pu**, Sonal Oswal, Gang Wang, Bimal Viswanath. ***IEEE S&P (Oakland) 2020, Online, May 2020***.
- "Multiview Clustering Based on Robust and Regularized Matrix Approximation", **Jiameng Pu**, Qian Zhang, Lefei Zhang, Bo Du. ***International Conference on Pattern Recognition, Cancun, Mexico, Nov 2016***.

Research Projects

Detecting GAN-generated Images at Virginia Tech

- Designed and built a custom hierarchical clustering algorithm for a detection system that can detect fake images generated from AI model — *Generative Adversarial Networks(GANs)* with upto 99.5% accuracy.
- Evaluated the detection system with 11 datasets of diverse content from 4 state-of-the-art GANs.
- Explored the blind detection of GAN-generated images by investigating image spaces and relevant correlation measures.

Investigating Attacks on Medical Image Diagnostics In Healthcare System at Virginia Tech

- Designed and implemented a GAN-based tool that can inject a specific disease condition to a patient's image, while preserving their identity.
- Demonstrated the attack feasibility on two popular biomedical image modalities — X-rays and retinal fundus images, and the effectiveness of progressive disease injection conditioned by disease stages.

Bot Detection with Limited Data at Virginia Tech

- Built a stream-based real-time bot detection system to complement with rule-based method to catch advanced bots.
- Developed a data synthesis method to enable effective model training with limited labeled data.
- Validated our system using real-world datasets from 3 different online services.
- Explored adversarial machine learning and transfer learning on bot detection.

Analyzing and Detecting DeepFake Videos in the Wild at Virginia Tech

- Collected a new in-the-wild DeepFake dataset comprising of DeepFake videos created and shared by the Internet community, e.g., YouTube, Bilibili and Reddit.
- Systematically evaluated and analyzed the performance of state-of-the-art deepfake detection schemes on the new DeepFake dataset.

Defending Against Trojan Attacks on Deep Text Models at Virginia Tech

- Re-engineered autoencoder to investigate NLP classifiers affected by backdoor attacks.
- Built initial prototype to extract word/phrase used for the attack.

Technical Skills

- **Languages:** *Python, Java, MATLAB, Javascript, C++, C, MySQL, Bash.*
- **Frameworks:** *Tensorflow, PyTorch, Keras, Scikit-Learn, DL models(CNNs, LSTMs, RNNs, etc.).*
- **Tools:** *Git, LaTeX, Unix systems.*
- **Certifications:** *Neural Networks and DL, Improving Deep Neural Networks, Structuring Machine Learning Projects (Deeplearning.ai)*