Jiameng Pu

Ph.D. Student

Virginia Tech
Department of Computer Science
✉ *jmpu@vt.edu*
🖱 *https://jmpu.github.io/*

Education

2017–Present **Ph.D. in Computer Science**, expected 2022.
Virginia Polytechnic Institute and State University, Blacksburg, VA, United States.
Research Interests: Data-driven security, machine learning.
Advisor: Dr. Bimal Viswanath

2013–2017 **B. Eng in Computer Science**.
Wuhan University, Wuhan, China

Research Experiences

2018–present **Graduate Research Assistant**.
Department of Computer Science, Virginia Tech, Blacksburg, VA, United States.
Research topic: Security and machine learning; Defending against threats posed by advances in ML; Using ML for better security.

2017–2018 **Graduate Research Assistant**.
Biocompleixty Institute, Virginia Tech, Blacksburg, VA, United States
Research topic: Understanding information propagation in complex networks using deep learning.

2016 **Data Science Intern**.
IBM China Development Labs, Wuhan, China
Research topic: Building machine learning tools for quality assessment in business scenarios.

2015–2016 **Undergraduate Research Assistant**.
State Key Lab of Software Engineering, Wuhan University, Wuhan, China
Research topic: Data clustering algorithms using matrix approximations.

Honors & Awards

2020 Visa Research Scholarship, awarded by IEEE S&P'20.

2019 Student Travel Grant, awarded by NDSS'19.

2014, 2015 National Endeavor Scholarships (given to top 5% students), awarded by Chinese Ministry of Education.

Publications

WWW'21 **A First Look at Deepfake Videos in the Wild: Analysis and Detection. (To appear)**
Jiameng Pu*, Neal Mangaokar*, Lauren Kelly, Parantapa Bhattacharya, Kavya Sundaram, Mobin Javed, Bolun Wang, and Bimal Viswanath.
WWW, Online, April 2021.

USENIX Security’21 **T-Miner: A Generative Approach to Defend Against Trojan Attacks on Deep Text Models. (To appear)**

Ahmadreza Azizi, Ibrahim Asadullah Tahmid, Asim Waheed, Neal Mangaokar, Jiameng Pu, Mobin Javed, Chandan K. Reddy, and Bimal Viswanath.

USENIX, Online, August 2021.

ACSAC’20 **NoiseScope: Spotting Deepfake Images in a Blind Setting.**

Jiameng Pu, Neal Mangaokar, Bolun Wang, Chandan Reddy, Bimal Viswanath.

ACSAC, Online, December 2020.

IEEE EuroS&P’20 **Jekyll: Attacking Medical Image Diagnostics Using Neural Translation.**

Neal Mangaokar, Jiameng Pu, Parantapa Bhattacharyam, Chandan Reddy, and Bimal Viswanath.

Euro S&P, Online, September 2020.

IEEE S&P’20 **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, and Bimal Viswanath.

IEEE S&P, Online, May 2020.

ICPR’16 **Multiview Clustering Based on Robust and Regularized Matrix Approximation.**

Jiameng Pu, Qian Zhang, Lefei Zhang, and Bo Du.

ICPR, Cancun, Mexico, July 2016.

Talks

2020 **Investigating Deepfakes: When Seeing is No Longer Believing.**

○ Virginia Tech, Department of Computer Science, January 2020

ACSAC’20 **NoiseScope: Spotting Deepfake Images in a Blind Setting.**

○ Online, December 2020

Project Code

ACSAC’20 **NoiseScope: Spotting Deepfake Images in a Blind Setting.**

○ https://github.com/jmpu/NoiseScope

Conference Experiences

ACSAC’20 **Annual Computer Security Applications Conference.**

Online, December 2020

CCS’20 **The ACM Conference on Computer and Communications Security.**

Online, November 2020

Euro S&P’20 **IEEE European Symposium on Security and Privacy.**

Online, September 2020

USENIX’20 **USENIX Security Symposium.**

Online, August 2020

IEEE S&P’20 **IEEE Symposium on Security and Privacy.**

Online, May 2020

CyberW 2020 **Workshop for Women in Cybersecurity Research.**

Online, March 2020

NDSS'19 **Network and Distributed System Security Symposium.**
San Diego, CA, United States, February 2019

Skills

Languages Python, Java, MATLAB, Javascript, C++, C, MySQL, Bash.

Frameworks Tensorflow, PyTorch, Hugging Face, DL models (Transformers, CNNs, LSTMs, RNNs, etc.)

Tools Git, LaTeX, Unix systems.