Xiang Cheng

+1(626)877-1252 | xiangcheng@vt.edu | https://xiangcheng.link | Blacksburg, VA, USA, 24060

Education

Virginia Tech — Blacksburg, VA
Ph.D. in Computer Science, Advisor: Yaling Yang — *Aug.2018 – May.2023(expected)*

University of Glasgow — Glasgow, UK
B.Eng., Electronic and Electrical Engineering, with Honors of the First Class — *Aug.2014 – May.2018*

University of Electronics Science and Technology of China — Chengdu, China
B.Eng., Electronic and Electrical Engineering, ranking 1/240 — *Aug.2014 – May.2018 (joint program)*

Work Experience

Meta, Software Engineer Intern — May 2022 – Aug 2022
Menlo Park, CA

Cross-App User Privacy Information Protection

- Designed and implemented an essential API for inner **privacy infrastructure** on iOS (Objective-C) to protect privacy data from leaking, which **accelerates** the infrastructure's adoption **by months**.
- Built **Android backend** detectors (Java & Kotlin) to detect potential **privacy violations** on Facebook and Facebook Lite, the detectors capture users' private information shared **cross-apps**.

Research Project

***Privacy-Friendly Digital Contact Tracing System**, Project Leader*

- Designed a digital contact tracing system utilizing geolocation information, the system protects users' privacy using **crypto algorithms** like homomorphic encryption, k-anonymity, and multi-party computation.
- Built an **Android app** with Reactive Native and a backend server using **Google Firebase**.
- Optimized the system to reduce the system's computation time **by 50%**.

***Robust GPS Spoofing Detection**, Project Leader*

- Proposed a GPS **spoofing detection system** working on off-the-shelf chipsets, the method **reduces the cost** of spoofing detection from thousands of dollars **to almost 0**, achieving **over 95%** detection accuracy.
- Built an Android data collection app (Java) and an analytic toolset.

Attack and Defense with Deep Learning

- Neural translation for attacks on the medical image domain: proposed and implemented custom generative neural networks (**GAN**) in adversarial settings to mislead medical diagnostics. The model is implemented with **TensorFlow** in python. The work revealed a realistic threat to the healthcare system posed by deep learning.
- Detecting GAN-synthesized deepfakes: developed a fingerprint-based clustering algorithm to **detect deepfake** images. The algorithm detects GAN-synthesized fake images with **99% accuracy** under an unsupervised setting.

Mobile Network Security

- Designed physical layer security solutions for mobile networks like 4G and 5G to help the network operate under extreme environments like interference and jamming.
- Built simulation frameworks (MATLAB) and proved the effectiveness of solutions with simulation results.

Technical Skills

Programming: Java/Python/Kotlin/MATLAB (proficient), C/C++/JavaScript/Objective-C (Skillful)
Tools & Frameworks: TensorFlow, Firebase, React Native, PyTorch, Node.js, Git, GNURadio

Publications

- **Cheng, X.**, Liu, S*., et al. Stars Can Tell: A Robust Method to Defend against GPS Spoofing Attacks using Off-the-shelf Chipset. **USENIX Security 2021**
- **Cheng, X.**, Yang, H., et al. 5G Physical Layer Resiliency Enhancements with NB-IoT Use Case Study. MILCOM 2023
- **Cheng, X.**, Yang, H., et al. Interoperable Privacy Preserving Digital Contact Tracing. Arxiv 2020
- Tian, J., Ren, Y., **Cheng, X.** Stratified Feature Sampling for Semi-Supervised Ensemble Clustering. IEEE Access 2019