YA (Athena) XIAO

Ph.D. student, Virginia Tech
✉ yax99@vt.edu
https://people.cs.vt.edu/yax99

RESEARCH INTERESTS

Neural network based solutions for software engineering domain, including code embedding, data-driven code suggestion, automatic vulnerability repair;

Software security including secure coding, finding vulnerabilities via static analysis;

Applied cryptography, neural cryptanalysis.

EDUCATION

Ph.D. student, Computer Science, Virginia Tech, Blacksburg, VA 2017 - Present

Tentative thesis: Methodologies for Automatic Code Generation for Repairing Complex Security Vulnerabilities

Thesis committee:

- ◇ Danfeng (Daphne) Yao, Professor, Elizabeth and James E. Turner Jr. '56 Faculty Fellow and CACI Faculty Fellow, Virigia Tech; (*Committee Chair*)
- ◇ Naren Ramakrishnan, Professor, Thomas L. Phillips Professor of Engineering, Virginia Tech;
- ◇ Matthew Hicks, Assistant Professor, Virginia Tech;
- ◇ Xinyang Ge, Researcher, Microsoft Research;
- ◇ Patrick Drew McDaniel, Professor, William L. Weiss Professor of Information and Communications Technology, PSU;

M.S., Information Security, Beijing University of Posts and Telecommunications (BUPT) 2014 - 2017

Thesis: Security Cryptanalysis of Lightweight Block Cipher (in Chinese).

B.S., Accunting, Beijing University of Posts and Telecommunications (BUPT) 2010 - 2014

Minor in *Information Security*; ranked 1/90 in the course *Modern Cryptography.*

HONORS AND AWARDS

BitShares Fellowship, Virginia Tech, Blacksburg, VA	2019
Member of the Honor Society of Phi Kappa Phi (GPA top 10 %), Virginia Tech, Blacksburg, VA	2018
National Scholarship, China	2015
University-level Scholarship, BUPT, Beijing, China	2011, 2014, 2016

RESEARCH EXPERIENCE

Research Intern

- Program Analysis Group, Oracle Labs, Brisbane, Australia June - August, 2019

  Working with Dr. Cristina Cifuentes (Senior Director of Research & Development in Oracle Labs Australia), and Paddy Krishnan (Director, Research at Oracle Labs Australia)

  Developed a static analyzer based on IFDS framework on top of LLVM to screen Java cryptographic API misuses. It achieves high precision and good scalability on large scale projects.

Research Assistant

Computer Science Department, Virginia Tech, Blacksburg, VA *August 2017 - present*

Research Projects:

- **Neural Network Based Code Repair Guided by Program Analysis Insights.**

  We design and comprehensively compare the neural-network-based methodologies to model Java security API usage. We design the program-analysis-guided embedding strategies to produce the dependence-aware code embedding. We develop a learning based code suggestion engine to suggest the correct API usage based on multiple data dependence paths extracted by program analysis.

- **Neural Cryptanalysis for CPS Ciphers**

  We invent an black-box security evaluation approach for cipher algorithms through deep learning. We measure the strength of CPS proprietary ciphers by learning its plaintext-ciphertext mapping with neural networks. We quantifya cipher strength by how difficult it can be learned.
- **High Precision Detection of Cryptographic Vulnerabilities in Java Programs**

  We design a static analyzer to detect Java cryptographic API misuses through backward inter-procedrual context-, field-sensitivy dataflow analysis. This tool, refined by our heuristics designed for cryptography code, achieves high precision with no or few false positives and low runtime.

Research Assistant

Beijing University of Posts and Telecommunications, Beijing, China *June 2014 - March 2017*

Participated Projects:

◇ Cryptanalysis of Lightweight Block Ciphers. We analyzed the security strength of lightweight block cipher SIMON and SIMECK family through differential and impossible differential cryptanalysis.
◇ Key Management Protocol of Heterogeneous Networks Composed of Wireless Sensor Networks (WSNs) and Vehicular Ad-hoc Networks (VANETs).
◇ Encryption and Authentication System Design for Smart Grids.

PUBLICATIONS

1. **Ya Xiao**, Md Salman Ahmed, Wenjia Song, Xinyang Ge, Bimal Viswanath, Danfeng (Daphne) Yao. "Embedding Code Contexts for Cryptographic APISuggestion: Methodologies and Comparisons." *(under submission).*

2. Md Salman Ahmed, **Ya Xiao**, Kevin Z. Snow, Gang Tan, Fabian Monrose, Danfeng (Daphne) Yao. "Methodologies for Quantifying (Re-)randomization Security and Timing under JIT-ROP." *The 27th ACM Conference on Computer and Communications Security (CCS'20)*

3. **Ya Xiao**, Yang Zhao, Nicholas Allen, Nathan Keynes, Danfeng (Daphne) Yao, Cristina Cifuentes. "Industrial Experience of Finding Cryptographic Vulnerabilities in Large-scale Codebases." *arXiv preprint arXiv:2007.06122 (2020).*

4. Yuan Luo, **Ya Xiao**, Long Cheng, Guojun Peng, and Danfeng Daphne Yao. "Deep Learning-Based Anomaly Detection in Cyber-Physical Systems: Progress and Opportunities." arXiv preprint arXiv:2003.13213 (2020).

5. Ying Zhang, Md Mahir Asef Kabir, **Ya Xiao**, Danfeng (Daphne) Yao, Na Meng. "Data-Driven Vulnerability Detection and Repair in Java Code." *(under submission).*

6. Sazzadur Rehaman, **Ya Xiao**, Sharmin Afrose, Fahad Shaon, Ke Tian, Miles Frantz1, Murat Kantarcioglu and Danfeng (Daphne) Yao. "CryptoGuard: High Precision Detection of Cryptographic Vulnerabilities in Massive-sized Java Projects." *The 26th ACM Conference on Computer and Communications Security (CCS'19).* London, UK, November 11-15, 2019. (Acceptance rate: 16%)

7. **Ya Xiao**, Qingying Hao and Danfeng (Daphne) Yao. "Neural Cryptanalysis: Metrics, Methodology, andApplications in CPS Ciphers." *The 2019 IEEE Conference on Dependable and Secure Computing (IDSC' 19).* Hangzhou, China, November 18-20, 2019.

8. Xiaodong Yu, **Ya Xiao**, Danfeng (Daphne) Yao and Kirk Cameron. "Comparative Measurement of Cache Configurations Impacts on Cache Timing Side-Channel Attacks." *The 12th USENIX Security Workshop on Cyber Security Experimentation and Test (CSET '19).* Santa Clara, CA, USA, August 12, 2019, 2019. (Acceptance rate: 31.1%)

9. **Ya Xiao**, Shihui Zheng and Bin Sun. "Trusted GPSR Protocol without Reputation Faking in VANET". *The Journal of China Universities of Posts and Telecommunications*, Vol.22, No.5, pp. 22-55, 2015. (EI Compendex; DOI: 10.1016/S1005-8885(15)60676-8)

Tutorials

1. **Ya Xiao**, Miles Frantz, Sharmin Afrose, Sazzadur Rahaman, Danfeng (Daphne) Yao. "Principles and Practices of Secure Cryptographic Coding in Java". *2020 IEEE Secure Development Conference (SecDev20).* September, 2020

Posters

1. Salman Ahmed, **Ya Xiao**, Gang Tan, Kevin Snow, Fabian Monrose, and Danfeng (Daphne) Yao. "Methodologies for Quantifying (Re-) Randomization Security and Timing under JIT-ROP." *In Network and Distributed Systems Security (NDSS) Symposium 2020*, San Diego, CA, USA.

2. Sazzadur Rahaman, **Ya Xiao**, Sharmin Afrose, Ke Tian, Miles Frantz, Danfeng (Daphne) Yao, Na Meng, Barton P. Miller, Fahad Shaon, Murat Kantarcioglu. "Deployment-quality and Accessible Solutions for Cryptography Code Development." *2019 IEEE Symposium on Security and Privacy (IEEE S&P'19).* San Francisco, CA, USA . May, 2019.

3. **Ya Xiao** and Danfeng (Daphne) Yao. "Automatic Patch Generation for Security Functional Vulnerabilities with GAN". *2018 IEEE Secure Development Conference (SecDev18).* Cambridge, MA. September, 2018.

Media Reports

1. CryptoGuard work was featured in Communications of the ACM. Jul. 2020. https://cacm.acm.org/news/246385-a-tool-for-hardening-java-crypto/fulltext

TEACHING EXPERIENCE

Teaching Assistant, Virginia Tech

CS 4264 Principles of Computer Security (*taught by Prof. Mathew Hicks*) Fall 2017

Course covering topics in cryptography, app security, network security, web security and forensics

Teaching Assistant, BUPT

Modern Cryptography (*taught by Prof. Yixian Yang and Prof. Shihui Zheng*) Spring 2015, 2016

National-level quality course in China

Academic Services

- Reviewer: IEEE Transactions on Dependable and Secure Computing (TDSC), Defence Science Journal (DSJ)

INCLUSIVE EXCELLENCE ACTIVITIES

Assistant for The 2020 Individualized Cybersecurity Research Mentoring Workshop (iMentor 2020)
Assistant of The 2020 Workshop for Women in Cybersecurity Research (CyberW 2020)
Member of Association of Women in Computing (AWC) at Virginia Tech. August 2018 - Present
Volunteer for the weekly event Coding with the Elderly in Blacksburg. August 2018 - Present