Binbin Zhao

binbin.zhao@gatech.edu
HomePage : https://www.bbge.org/ (+1) 470-309-9987

EDUCATION

Ph.D. Candidate, Georgia Institute of Technology 2019-2023 (expected)
Electrical and Computer Engineering, GPA: 4.00/4.00
Advisor: Prof. Raheem Beyah & Prof. Shouling Ji

Master of Science, Georgia Institute of Technology 2019-2022
Electrical and Computer Engineering, GPA: 4.00/4.00
Advisor: Prof. Raheem Beyah & Prof. Shouling Ji

Bachelor of Engineering, Zhejiang University 2014-2018
Computer Science and Technology, GPA: 3.77/4.00, Major GPA: 3.84/4.00
Advisor: Prof. Shouling Ji

RESEARCH INTEREST

I am interested in real-world computer security problems, especially in IoT security, fuzzing, and data-driven security.

PUBLICATIONS

- Jiacheng Xu, Xuhong Zhang, Shouling Ji, Yuan Tian, **Binbin Zhao**, Qinying Wang, Peng Cheng, Jiming Chen, "Anonymity", Submitted to CCS, 2023.
- **Binbin Zhao**, Shouling Ji, Jiacheng Xu, Yuan Tian, Qinying Wang, Qiuyang Wei, Chenyang Lyu, Xuhong Zhang, Changting Lin, Jingzheng Wu, Reheem Beyah, "One Bad Apple Spoils the Barrel: Understanding the Security Risks Introduced by Third-Party Components in IoT Firmware", Submitted to IEEE Transactions on Dependable and Secure Computing. [paper]
- Qinying Wang, Boyu Chang, Shouling Ji, Xuhong Zhang, Yuan Tian, **Binbin Zhao**, Gaoning Pan, Chenyang Lyu, Wenhai Wang, Reheem Beyah, "Anonymity", Submitted to IEEE S&P & Under Major Revision, 2023.
- **Binbin Zhao**, Shouling Ji, Xuhong Zhang, Yuan Tian, Qinying Wang, Yuwen Pu, Chenyang Lyu, Reheem Beyah, "UVScan: Detecting Third-Party Component Usage Violations in IoT Firmware", 32nd USENIX Security Symposium, 2023. (CCF-A)
- Chenyang Lyu, Jiacheng Xu, Shouling Ji, Xuhong Zhang, Qinying Wang, **Binbin Zhao**, Wei Cao, Alex X. Liu, Reheem Beyah, "MINER: A Hybrid Data-Driven Approach for REST API Fuzzing", 32nd USENIX Security Symposium, 2023. [paper] (CCF-A)
- Shouling Ji, Qinying Wang, Anying Chen, **Binbin Zhao**, Tong Ye, Xuhong Zhang, Jingzheng Wu, Yun Li, Jianwei Yin, Yanjun Wu, "State-of-the-Art Survey of Open-source Software Supply Chain Security", Journal of Software, 2022. [paper] (CCF-T1)
- **Binbin Zhao**, Shouling Ji, Jiacheng Xu, Yuan Tian, Qinying Wang, Qiuyang Wei, Chenyang Lyu, Xuhong Zhang, Changting Lin, Jingzheng Wu, Reheem Beyah, "A Large-Scale Empirical Analysis of the Vulnerabilities Introduced by Third-party Components in IoT Firmware", ISSTA, 2022. (CCF-A) [paper]
- Chenyang Lyu, Hong Liang, Shouling Ji, Xuhong Zhang, **Binbin Zhao**, Meng Han, Yun Li, Zhe Wang, Wenhai Wang, Reheem Beyah,"SLIME: Program-sensitive Energy Allocation for Fuzzing", ISSTA, 2022. (CCF-A) [paper]
- Chenyang Lyu, Shouling Ji, Xuhong Zhang, Hong Liang, **Binbin Zhao**, Kangjie Lu, Reheem Beyah, "EMS: History-Driven Mutation for Coverage-based Fuzzing", NDSS, 2022. (CCF-A) [paper]
- Qinying Wang, Shouling Ji, Yuan Tian, Xuhong Zhang, **Binbin Zhao**, Yuhong Kan, Zhaowei Lin, Changting Lin, Shuiguang Deng, Alex X. Liu, Reheem Beyah,

"MPInspector: A Systematic and Automatic Approach for Evaluating the Security of IoT Messaging Protocols", 30th USENIX Security Symposium, 2021. (CCF-A) [paper]

- **Binbin Zhao**, Shouling Ji, Wei-Han Lee, Changting Lin, Haiqing Weng, Jingzheng Wu, Pan Zhou, Liming Fang, Reheem Beyah, "A Large-scale Empirical Study on the Vulnerability of Deployed IoT Devices", IEEE Transactions on Dependable and Secure Computing, 2020. (CCF-A) [paper]
- Haiqin Weng*, **Binbin Zhao***, Shouling Ji, Jianhai Chen, Ting Wang, Qinming He, Raheem Beyah, "Towards Understanding the Security of Modern Image Captchas and Underground Captcha-solving Services", Big Data Mining and Analytics, 2019. [paper] (CCF-T2)
- **Binbin Zhao***, Haiqin Weng*, Shouling Ji, Jianhai Chen, Ting Wang, Qinming He, Raheem Beyah, "Towards Evaluating the Security of Image CAPTCHA in the Wild", Proceedings of the 11th ACM Workshop on Artificial Intelligence and Security, in conjunction with the CCS, 2018. [paper]

RESEARCH EXPERIENCE

- **CAP Lab, Georgia Institute of Technology** Aug. 2019 - Present
  Research Assistant, Advised by Prof. Raheem Beyah Atlanta, GA

  Project: Detecting Third-Party Component Usage Violations in IoT Firmware

  1. Proposed UVScan, the first automated and scalable system to detect third-party component usage violations in firmware.
  2. Conducted a large-scale analysis on 4,545 firmware images and detected 36,097 usage violations.

  Project: A Large-Scale Empirical Analysis of the Vulnerabilities Introduced by Third-party Components in IoT Firmware

  1. Proposed FirmSec, the first automated and scalable framework to analyze the third-party components used in firmware and identify the corresponding vulnerabilities.
  2. Constructed so far the largest firmware dataset, which includes 34,136 firmware images, and conducted the first large-scale analysis of the vulnerable third-party component problem in firmware.

- **NESA Lab, Zhejiang University** Jun. 2018 - Jul. 2019
  Research Fellow, Advised by Prof. Shouling Ji Hangzhou, China

  Project: A Large-Scale Empirical Analysis of the Vulnerabilities Introduced by Third-party Components in IoT Firmware

  1. Embarked on a multi-aspect comparative study on five IoT Search Engines, e.g., Shodan, Censys, Zoomeye, Fofa, NTI.
  2. Collected millions of exposed devices from six kinds of IoT devices, e.g., Router, Webcam, Printer, Miner, Medical devices, and Industrial Control Systems (ICS).
  3. Succeeded in testing million-level devices in three dimensions, including weak password usage, nearly 100 N-days vulnerabilities testing, and the long-term longitudinal study.
  4. Proposed deceptive defense technique to protect the vulnerable IoT devices.

- **NESA Lab at Zhejiang University** Jul. 2017 - Apr. 2018
  Research Assistant, Advised by Prof. Shouling Ji Hangzhou, China

  Project: Towards Evaluating the Security of Image CAPTCHA in the Wild

  1. Attacked three kinds of Image Captchas by using machine learning, including Selection-based, Slide-based and Click-based Image Captchas.
  2. Conducted a measurement study on the underground market of captcha-solving service.

3. Proposed several methods against the attack, such as adding adversarial noises to original captcha.
4. Reported one high-risk and one medium-risk vulnerabilities to NetEase Security Response Center.
5. Reported two medium-risk vulnerabilities to Tencent Security Response Center.

WORKING EXPERIENCE

- **Interactive Entertainment Group (IEG), Tencent** Aug. 2018 - Jun. 2018
  Software Development Engineer Intern Shenzhen, China

TEACHING EXPERIENCE

- **Zhejiang University** | Prof. Janice Regan Sept. 2017 - Feb. 2018
  Teaching Assistant Hangzhou, China
  Object-oriented Programming (C++)

ACADEMIC SERVICE

Program Committee:
- **IEEE Symposium on Security and Privacy Poster Session** 2023

SELECTED TALKS

Detecting Third-Party Component Usage Violations in IoT Firmware
Invited talk at USENIX Security Anaheim, CA, Aug. 2023

A Large-Scale Empirical Analysis of the Vulnerabilities Introduced by Third-party Components in IoT Firmware
Invited talk at IIE, Chinese Academy of Sciences Virtually, Aug. 2022
Invited talk at ISSTA Virtually, July 2022

SELECTED AWARDS

- **IEEE Symposium on Security and Privacy Student Grant** 2022
- **ACM SIGSOFT CAPS Support for ICSE** 2022
- **NDSS Student Grant** 2022
- **Outstanding Exchange Student Scholarship**, Zhejiang University 2016

REFERENCES

Raheem A. Beyah Professor, Dean and Southern Company Chair, Georgia Tech
Shouling Ji Professor, Zhejiang University
Yuan Tian Assistant Professor, UCLA