

Xu He

✉ xhe6@gmu.edu
🌐 sites.google.com/view/hexu
🐙 github.com/Viewer-HX
☎ 571-685-3344

EDUCATION

- **PhD, Information Technology - George Mason University** Sep 2019 - Dec 2024 (expected)
Research - Software Security & Analysis; Network Optimization; AI Security. GPA: 4.0/4.0
- **MS, Computer Science - Nanjing University of Posts & Telecom.** Sep 2016 - May 2019
Concentration - Machine Learning; Social Media Data Mining. GPA: 87.9/100
- **BS, Communication Engineering - Nanjing University of Posts & Telecom.** Sep 2012 - Jun 2016
Outstanding Thesis Award; Honors College Graduates.(Top 5/77) GPA: 87.5/100

EXPERIENCE

- **Center for Secure Information System (CSIS), GMU** Fairfax, VA
Graduate Research Assistant (Advisor: Dr. Kun Sun) Sep 2019 - Present
 - **Automatic Program Repair via Static Analysis and Formal Method:** Automated vulnerability detection and patch generation through static analysis and constraint solving on patched and unpatched program pairs.
 - **Security Impact Analysis of Compilation Optimization:** Explore the security impact of compilation optimization on software by combining program analysis and deep learning techniques, which can benefit downstream security analysis tasks, such as compiler provenance identification, security patch detection, and compiler-induced bug detection and repair.
 - **Network Optimization by Tuning Buffer Parameters:** Improve the network performance by automatically tuning buffers in the network stack based on the Reinforcement Learning techniques.
- **NIO USA Inc.** San Jose, CA
Security R&D Internship (SOA) May 2022 - Aug 2022
 - **Risk Scenarios Analysis of In-Vehicle Software:** Summarize potential security threats and investigate corresponding solutions in the in-vehicle software services and assets.
 - **IAM Plugin:** Implement the authentication procedure between remote services, including service discovery and security information encryption and decryption.

Automotive Cybersecurity Software Developer (PhD Internship) May 2023 - Aug 2023

 - **Intrusion Detection System (IDS) of Remote Vehicle Security Services:** (1) Design and implement the IDS system and the log I/O API on the cloud end. (2) Improve the retrieval efficiency of the rule engine based on real-time data streaming.

SKILLS SUMMARY

- **Languages:** Python, C, C++, Rust, Latex, Matlab.
- **Program Analysis:** KLEE, Z3, LLVM, Angr, Joern.
- **Depp Learning:** Pytorch, Fairseq, Tensorflow.
- **Expertise:** Static Analysis, Symbolic Execution, Deep Learning, Linux Network Stack.

SERVICES

- **Conference Reviewer (sub/external) (2020-2024):** CCS; Usenix Security; NDSS; INFOCOM; DSN; ACSAC; AsiaCCS; CNS; MILCOM; ICICS.
- **Journal Reviewer:** ACM: DTRAP; Springer: Wireless Networks; Elsevier: Computer Communications; MDPI: Sensors /ISPRS IJGI/MAKE/Entropy.
- **Artifact Reviewer (2023-2024):** NDSS; ACSAC .
- **Vulnerability Reporter:** RUSTSEC-ID (2023-0046, 2023-0047) and CVE (2022-47085)

AWARDS

- **Honorable Mention Award**, American Mathematical Contest In Modeling (COMAP), Feb. 2015.
- **Student Grant Award**, INFOCOM 2022, Apr. 2022.
- **Doctoral Research Scholarship**, George Mason University, Jun. 2023.

1. **BinGo: Identifying Security Patches in Binary Code with Graph Representation Learning**
Xu He, Shu Wang, Pengbing Feng, Xinda Wang, Shiyu Sun, Qi Li, Kun Sun
ACM ASIA Conference on Computer and Communications Security (ASIACCS 2024)
(Acceptance Rate: 65/301 = 21%)
 2. **What IF Is Not Enough? Fixing Null Pointer Dereference With Contextual Check**
Yunlong Xing, Shu Wang, Shiyu Sun, **Xu He**, Kun Sun, Qi Li
USENIX Security Symposium (USENIX Security 2024)
(Acceptance Rate: 98/515 = 19.0%)
 3. **BinProv: Binary Code Provenance Identification without Disassembly**
Xu He, Shu Wang, Pengbin Feng, Kun Sun, Haining Wang, Qi Li, Songqing Chen
The 25th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2022)
(Acceptance Rate: 35/139 = 25.1%)
 4. **Consistency is All I Ask: Attacks and Countermeasures on the Network Context of Distributed Honeypots**
Songsong Liu, Pengbin Feng, Jiahao Cao, **Xu He**, Tommy Chin, Kun Sun, and Qi Li
The 19th Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA 2022)
(Acceptance Rate: 11/39 = 28.2%)
 5. **Auter: Automatically Tuning Multi-layer Network Buffers in Long-Distance Socks Networks**
Xu He, Jiahao Cao, Shu Wang, Kun Sun, Lisong Xu, Qi Li
The 41st IEEE International Conference on Computer Communications (INFOCOM 2022)
(Acceptance Rate: 225/1129 = 19.9%) (**Student Grant Award**)
 6. **When the Differences in Frequency Domain are Compensated: Understanding and Defeating Modulated Replay Attacks on Automatic Speech Recognition**
Shu Wang, Jiahao Cao, **Xu He**, Kun Sun, Qi Li
The 27th ACM Conference on Computer and Communications Security (CCS 2020)
(Acceptance Rate: 121/715 = 16.9%)
 7. **RusTEE: Developing Memory-Safe ARM TrustZone Applications**
Shengye Wan, Mingshen Sun, Kun Sun, Ning Zhang, **Xu He**
2020 Annual Computer Security Applications Conference (ACSAC 2020)
(Acceptance Rate: 70/302 = 23%)
 8. **An Automatic Annotation Method for Discovering Semantic Information of Geographical Locations from Location-Based Social Networks**
Zhiqiang Zou, **Xu He**, A-xing Zhu
2019 ISPRS International Journal of Geo-Information
 9. **Enhancing the Impression on Cities: Mining Relations of Attractions with Geo-Tagged Photos**
Zhiqiang Zou, **Xu He**, Xingyu Xie, Qunying Huang
2018 IEEE Symposia and Workshops on Ubiquitous, Autonomic and Trusted Computing (UIC-ATC 2018)
 10. **Sparse Representation of Sensor Network Signals Based on the K-SVD Algorithm**
Zhiqiang Zou, **Xu He**, Yinxia Wang, Jiagao Wu
2018 ACM International Conference on Modelling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM 2018)
- * **TYPEPULSE: Detecting Type Confusion Bugs in Rust Programs**
Hongmao Chen, **Xu He**, Shu Wang, Xiaokuan Zhang, Kun Sun
Under Review, Submitted to USENIX Security Symposium (USENIX Security 2024)
- * **PathFix: Automated Program Repair with Expected Path**
Xu He, Shu Wang, Qi Li, Kun Sun
Under Review, Submitted to ACM Conference on Computer and Communications Security (ACM CCS 2024)