Xu He

xhe6@gmu.edu
xuhe.info
github.com/Viewer-HX
571-685-3344

Education

- **PhD, Information Technology - George Mason University** Sep 2019 - Dec 2024 (expected)
  Research - Software Security & Analysis; Deep Learning; Network Optimization. *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*
  - **Security Impact of Compilation on Binary**: Research the impact of compilation optimization on binary. Integrate program analysis and NLP techniques to enhance security analysis tasks, including compiler provenance identification, security patch detection, and detection and repair of compiler-induced bugs.
  - **Automatic Program Repair**: Develop a system for automated patch generation using static analysis and symbolic execution. This involved exploring possible correct execution paths to replace buggy ones and solving constraints to generate patches.
  - **Network Performance Optimization**: Improve the network performance by automatically tuning buffer parameters in the network stack based on Reinforcement Learning.
- **NIO USA Inc.** San Jose, CA
  Security R&D Intern (SOA) *May 2022 - Aug 2022*
  - **TARA Analysis**: Investigate potential security threats, risks, and solutions of in-vehicle software services.
  - **IAM Development**: Implement the Identity and Access Management plugin of in-vehicle software services.

  Automotive Cybersecurity Software Developer (PhD Intern) *May 2023 - Aug 2023*
  - **IDS Development and Improvement**: (1) Design and implement the Intrusion Detection System (IDS) of remote vehicle security services. (2) Redesign the rule engine of IDS to improve its retrieval efficiency.
- **VISA Inc.** Ashburn, VA
  Sr.Data Scientist (Cybersecurity), Intern *May 2024 - Aug 2024*
  - **Generative AI Application in Cybersecurity**: Use Generative AI techniques to automate cybersecurity processing flow.

Skills Summary

- **Expertise**: Static Analysis, Deep Learning, Linux Network Stack.
- **Program Analysis**: KLEE, CodeQL, Z3, LLVM, Angr, Joern.
- **Deep Learning**: Pytorch, Fairseq, HuggingFace, Candle.
- **Languages**: Python, C, C++, Rust, Bash, Matlab.

Services

- **Conference Review (include subreview) (2020-2024)**: CCS; Usenix Security; NDSS; INFOCOM; DSN; ACSAC; AsiaCCS; CNS; MILCOM; ICICS.
- **Journal Review**: IEEE TIFS; ACM DTRAP; Springer WINE; Elsevier Computer Communications.
- **Artifact Review (2023-2024)**: NDSS; ACSAC; CCS.
- **Vulnerability Report**: 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.

Publication

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 Shadowsocks 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 ACM Conference on Computer and Communications Security (ACM CCS 2024)

* **PathFix: Automated Program Repair with Expected Path**
Xu He, Shu Wang, Kun Sun
Under Review, Submitted to the Annual Computer Security Applications Conference (ACSAC 2024)