HENGKAI YE

Ph.D. Candidate
College of Information Sciences and Technology
The Pennsylvania State University

hengkai@psu.edu
765-772-8417
https://hengkai-ye.github.io/
E338 Westgate Building
University Park, PA 16802

RESEARCH INTERESTS

Software and System Security: My research focuses on identifying new exploitation methods and exploring novel attack surfaces in software and system. I employ program-analysis techniques (e.g., control-flow analysis, data-flow analysis, and fuzzing) across my research projects.

LLM and Agent Security: I am leading projects in evaluating and mitigating security issues in LLM-based applications. I am also interested in leveraging LLMs and agents to address conventional security tasks, such as vulnerability detection and patching.

EDUCATION

The Pennsylvania State University, State College, PA, USA — May 2022 - Present

Ph.D. in Informatics
Advisor: Hong Hu

Purdue University, West Lafayette, IN, USA — Aug 2020 - May 2022

M.S. in Computer and Information Technology

Huazhong University of Science and Technology, Wuhan, China — Sept 2016 - Jun 2020

B.E. in Information Security

PUBLICATIONS

Refereed Conference Proceedings

[1] **SACK: Systematic Generation of Function Substitution Attacks Against Control-Flow Integrity**.
Zhechang Zhang, Hengkai Ye, and Hong Hu.
In *Proceedings of the Annual Network and Distributed System Security Symposium (**NDSS**)*, San Diego, CA, February 2026.

[2] **Too Subtle to Notice: Investigating Executable Stack Issues in Linux Systems**.
Hengkai Ye and Hong Hu.
In *Proceedings of the Annual Network and Distributed System Security Symposium (**NDSS**)*, San Diego, CA, February 2025.

[3] **VIPER: Spotting Syscall-Guard Variables for Data-Only Attacks**.
Hengkai Ye, Song Liu, Zhechang Zhang, and Hong Hu.
In *Proceedings of the USENIX Security Symposium (**Security**)*, Anaheim, CA, August 2023.

[4] **BET: black-box efficient testing for convolutional neural networks**.
Jialai Wang, Han Qiu, Yi Rong, Hengkai Ye, Qi Li, Zongpeng Li, and Chao Zhang.
In *Proceedings of the ACM International Symposium on Software Testing and Analysis (**ISSTA**)*, July 2022.

Journal Articles

[5] **Interpreting Deep Learning-based Vulnerability Detector Predictions Based on Heuristic Searching**.
Deqing Zou, Yawei Zhu, Shouhuai Xu, Zhen Li, Hai Jin, and Hengkai Ye.
In *ACM Transactions on Software Engineering and Methodology (**TOSEM**)*, 2021.

Others

[6] **Executable Stack Issues in Software Transformation (Accepted As Talk)**.
Hengkai Ye and Hong Hu.
In *Workshop on Forming an Ecosystem Around Software Transformation (**FEAST**)*, October 2024.

[7] **One Flip is All It Takes: Identifying Syscall-Guard Variables for Data-Only Attacks**.
Hengkai Ye, Hong Hu, Song Liu, and Zhechang Zhang.
In *Black Hat Asia Briefings*, April 2024.

Under Review

[8] **TrustDesc: Preventing Tool Poisoning in LLM Applications via Trusted Description Generation**.
Hengkai Ye, Zhechang Zhang, Jinyuan Jia, and Hong Hu.

[9] **NCFuzz: Configuration-guided Network Service Fuzzing**.
Xuesong Bai, Hengkai Ye, Shenghan Zheng, Fenglu Zhang, Hong Hu, and Zhou Li.

HONORS AND AWARDS

Student Travel Grant, USENIX Security	2023
Mingde Scholarship, Huazhong University of Science and Technology	2019
Freshman Scholarship, Huazhong University of Science and Technology	2016

ACTIVITIES

Poster Program Committee Member

ACM Conference on Computer and Communications Security (CCS)	2025

Artifact Evaluation Committee Member

Network and Distributed System Security Symposium (NDSS)	2025, 2026

External Reviewer

USENIX Security Symposium (Security)	2025, 2026
Network and Distributed System Security Symposium (NDSS)	2023, 2024, 2025, 2026
ACM Conference on Computer and Communications Security (CCS)	2022, 2024, 2025

Reviewer

[Springer Journal] Cybersecurity

Teaching Assistant

IST 454 Computer and Cyber Forencis	Fall 2022

OPEN SOURCE CONTRIBUTION

BadAss: Demonstration of the BadAss issue [2]
https://github.com/PSU-Security-Universe/badass

Viper. A tool for identifying syscall-guard variables [3]
https://github.com/PSU-Security-Universe/viper

Data-only attacks. A list of data-only attacks [3]
https://github.com/PSU-Security-Universe/data-only-attacks