HONGWEI WU

(765)714-9380 wu1685@purdue.edu hwu71 hwu71.github.io Hongwei-Wu

EDUCATION

Purdue University | Department of Computer Science — **West Lafayette, IN**
Ph.D. in Computer Science — *August 2020 - May 2026 (Expected)*

Binghamton University, SUNY | Watson College of Engineering — **Binghamton, NY**
M.S. in Computer Science (Distinguish Graduate Student) — *August 2018 - May 2020*

Renmin University of China | School of Information — **Beijing, China**
B.S. in Information Security — *September 2015 - June 2019*

TECHNICAL SKILLS

- Expertise: Program Analysis, Binary Analysis, Reverse Engineering, Decompiler, Embedded System, Large Language Model, Fuzzing
- Languages: Python, Assembly, C/C++, JavaScript, HTML
- Tools: angr, IDA pro, Ghidra, Intel Pin, LLVM, GDB, syzkaller

RESEARCH EXPERIENCE

Purdue University — **West Lafayette, IN**
Research Assistant advised by Dr. Antonio Bianchi — *August 2020 - Present*

- Developed *VeriBin*, an adaptive system designed to verify patch safety without requiring source code by employing symbolic execution to detect patch-introduced modifications, adaptively query analysts for these modifications, and verify whether the patch preserves the original functionality. Achieved 93% accuracy with no false positives on a dataset of 86 samples.
- Applied and expanded *VeriBin* in DARPA's Assured Micropatching Program to verify binary-level micro-patches for legacy binary systems without access to the source code (Cummins engine ECUs, NASA Lunar rovers, and power grid infrastructures, etc.), by enhancing the symbolic execution of ***angr*** for various embedded architectures (ARM, PowerPC, etc.) and collaborating with industry partners to integrate the tool into strategic frameworks.
- Spearheaded the development of *Artiphishell* for DARPA's AI Cybersecurity Challenge with team Shellphish, creating an LLM-based Cyber Reasoning System that autonomously identifies, analyzes, and patches software vulnerabilities, playing a key role in validating LLM-generated patches to ensure they addressed vulnerabilities without introducing new ones. Our team won a $2 million cash award during the semifinals, uniquely patched a vulnerability, and advanced to the final phase (7 out of 42 teams).

Binghamton University — **Binghamton, NY**
Research Assistant advised by Dr. Aravind Prakash — *June 2019 - May 2020*

- Evaluated the effectiveness of debloating methods by implementing Intel Pin-based Pintools to measure runtime instruction execution and utilizing WinAFL to analyze code coverage of WinRAR using debloated libraries.
- Reproduced rowhammer attacks on machines with non-ECC DRAM to engender bit flips and designed an algorithm to generate a unique identifier for victim machines based on their unique bit-flipping patterns under rowhammer attack.

PUBLICATIONS

- **Hongwei Wu**, Jianliang Wu, Ruoyu Wu, Ayushi Sharma, Aravind Machiry, and Antonio Bianchi, "VeriBin: Adaptive Verification of Patches at the Binary Level" In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2025.