Yuhui Zhu

github.com/zhuyuhui97
yuhui.zhu@santannapisa.it
zhuyuhui97.github.io
Scuola Superiore Sant'Anna

Education

1. **Scuola Superiore Sant'Anna & Scuola IMT Alti Studi Lucca** Pisa, Italy
   Italian National PhD Program in Cybersecurity. *Dec. 2022 - Present*
   Supervisor: Alessandro Biondi (Scuola Superiore Sant'Anna, Pisa)

2. **Vrije Universiteit Amsterdam** Amsterdam, Netherlands
   Visiting PhD Student at VUSec Group. *Feb. 2025 - Aug. 2025*
   Supervisor: Cristiano Giuffrida

3. **University of Jinan - School of Information Science and Engineering** Shandong, China
   Master of Engineering - Computer Science. *Nov. 2019 - Jun. 2022*
   Supervisor: Zhenxiang Chen

4. **University of Jinan - School of Information Science and Engineering** Shandong, China
   Bachelor of Engineering - Computer Science. *Nov. 2015 - Jun. 2019*

Publications

1. **Yuhui Zhu**, Alessandro Biondi
   Exploiting Inaccurate Branch History in Side-Channel Attacks
   34th USENIX Security Symposium (USENIX Security 2025)
   [USENIX] [Artifact] [ArXiv]

2. Berenice Fernández Nieto, Daisy Romanini, **Yuhui Zhu**
   Cybersecurity Education Showdown: A Comparative Analysis of K-12 Education Systems in the United States, the European Union and China
   ITASEC - Italian Conference on CyberSecurity 2025
   [PDF@CEUR-WS]

3. **Yuhui Zhu**, Zhenxiang Chen, Qiben Yan, Shanshan Wang, Alberto Giaretta, Enlong Li, Lizhi Peng, Chuan Zhao, Mauro Conti
   Devils in the Clouds: An Evolutionary Study of Telnet Bot Loaders
   IEEE International Conference on Communications 2023
   [IEEE] [ArXiv]

4. Nasimul Hasan, Zhenxiang Chen, Chuan Zhao, **Yuhui Zhu**, Cong Liu
   IoT Botnet Detection framework from Network Behavior based on Extreme Learning Machine
   IEEE INFOCOM Workshop: BigSecurity 2022
   [IEEE]

5. Gang Zhang, Hao Li, Zhenxiang Chen, Lizhi Peng, **Yuhui Zhu**, Chuan Zhao
   AndroCreme: Unseen Android Malware Detection Based on Inductive Conformal Learning
   TrustCom 2021
   [IEEE]

6. Jingya Shen, Zhenxiang Chen, Shanshan Wang, **Yuhui Zhu**, Muhammad Umair Hassan
   DroidDetector: a traffic-based platform to detect android malware using machine learning
   Third International Workshop on Pattern Recognition 2018
   [SPIE]

CVEs

1. **CVE-2024-10929: Spectre-BSE attack on Cortex-A72/A73/A75.**
   CVE assigned by ARM. Identified a novel vulnerability leveraging an undocumented *bias-free* behavior in the Branch History Buffer (BHB) update mechanism, enabling hijacking of history-based branch prediction. Detailed in the USENIX Security 2025 paper. (Publication 1)
   [NVD] [ARM] [AMD]

Patents

1. **Android Application Testbench System Based on the Test Farm**
   Patent No. CN202110088425.2
2. **An Embedded Realtime Collector for Network Flows and Runtime Logs on Android OS**
   Patent No. CN202110111586.9
3. **Network Flow Collector for Encrypted Network Conversations on Android OS**
   Patent No. CN202110103856.1

Skills

1. **Languages**: English (Fluent), Chinese (Native).
2. **Programming**: C/C++, Python, Bash, Java (Android), Verilog, C#, Assembly (x86/ARM/MIPS).
3. **Embedded Systems**: Firmware development, microcontrollers, Bluetooth, LoRa, PCB design.
4. **Systems & Tools**: Linux kernel & driver programming, QEMU, iptables, Git, DPDK, eBPF.
5. **Security**: Microarchitecture vulnerabilities and mitigations, Binary analysis, exploit development, reverse engineering, HW&SW cross-platform debugging.

Honors and Awards

1. 1st class university scholarship in 2019, and other classes in 2016, 2018, 2020 and 2021.
2. Finalist prize in *Loongson Cup 1st National Student Computer System Capability Challenge.* *Sep. 2017*
3. 3rd prize in *14th Shandong Provincial Software Design Competition for University Students.* *Nov. 2016*
4. Finalist prize in *Inspur Cup 7th Shandong Provincial ACM-ICPC Programming Competition.* *Sep. 2016*

Projects

1. **Speculative Execution Vulnerabilities** *Mar. 2023 – Present*
   Group research project supervised by Prof. Alessandro Biondi.
   - Conducted reverse engineering of diverse CPU microarchitectures and systematically analyzed security-critical software components (OS kernels, language runtimes, browsers) to study vulnerabilities emerging at the interface between hardware and software security mechanisms.
   - Discovered undocumented microarchitectural behaviors and identified a series of previously unknown Spectre variants that exploit these behaviors (Publication 1).
   - Designed and implemented a suite of tools for automated testing and analysis of speculative execution vulnerabilities.
   - Developed proof-of-concept exploits using assembly and eBPF.

2. **Network-Flow-Based Mobile Malware Detection with Adaptive ML** *Nov. 2015 – Jul. 2022*
   Group research project supervised by Prof. Zhenxiang Chen in collaboration with Huawei Shield Lab.
   - Designed and implemented an *Android test farm* for massive automated metadata extraction, app execution, event injection, and network trace collection.
   - Developed infrastructure for *real-time data capture, processing, and classification* on high-speed backbone networks and edge routers.
   - Conducted research on *adaptive machine learning* for malware detection, including incremental learning, explainable DNNs, and model optimization. (Publication 4, 5, 6)

3. **Knowledge-Guided Detection and Attribution of IoT Botnets** *Sep. 2020 – Jul. 2022*
   Group research project supervised by Prof. Zhenxiang Chen in collaboration with Huawei Shield Lab.
   - Designed and implemented a *transport-layer honeycloud framework* for deploying multi-protocol honeypots and capturing infection traffic at scale.
   - Developed a *multi-architecture sandbox* for automated analysis of IoT botnet malware across diverse hardware platforms.
   - Investigated botnet malware *lineage and family attribution* by analyzing behavioral homology in infection patterns. (Publication 3)

4. **Bluetooth RGB LED Controller** *Apr. 2017 – Jan. 2018*
   - Implemented a framebuffer rendering engine for STM32/ESP32, leveraging DMA to minimize transfer intervals and achieve full-speed RGB LED refresh.
   - Developed Bluetooth Low Energy (BLE) and LoRa communication protocols for remote control.
   - Designed, prototyped, and tested a custom PCB.

5. **Bypassing NAT Detection in an Android Network Authenticator App** *Nov. 2017*
   - Used Magisk to hook internal app functions and bypass NAT detection by intercepting API calls.

6. **A 5-Stage Pipelined MIPS R3000 CPU in Verilog on an Altera FPGA** *Jun. 2017 – Sep. 2017*
   Loongson Cup – 1st National Student Computer System Challenge – contest submission.
   - Developed data hazard resolution logic, a floating-point coprocessor, and an instruction cache.
   - Created and adapted assembly test cases to validate functionality and performance.

7. **High-Performance DNS Mirror based on DPDK** *Jan. 2017 – May 2017*
   - Achieved high-throughput DNS without relying on full-scale TCP/IP stacks.

8. **Retail Store Support System** *Jun. 2016 – Aug. 2016*
   14th Shandong University Software Design Competition – contest submission.
   - Developed an Android–Node.js platform to manage procurement, inventory, and sales operations.

9. **Laundromat Platform** *Jun. 2016 – Aug. 2016*
   14th Shandong University Software Design Competition – contest submission.
   - Enhanced the UART-over-cellular control platform by improving communication and heartbeat monitoring logic on both server and client sides, and refined the user interface for payment processing and status tracking.