Haotian Deng

PROGRAM ANALYSIS · SYSTEMS & SOFTWARE SECURITY · AI FOR SECURITY

h.deng@std.uestc.edu.cn

PUBLICATIONS

Underline denotes first / lead author.

[1] **Haotian Deng**, Meng Hao, Hanxiao Chen, Xinyuan Qian, Guowen Xu, Hongwei Li, Chaoshun Zuo. "Beyond Sensitive APIs: Detecting Access Control Flaws at Sensitive Callsites in Android Firmware." In Proceedings of the Network and Distributed System Security Symposium (**NDSS**), 2027.

[2] **Haotian Deng**, Hongwei Li, Hanxiao Chen, Meng Hao, Pengzhi Xing, Jia Hu, Rui Zhang, Wenbo Jiang. "SecInfer: Secure and Efficient Model Inference on Vertically Partitioned Data." In Proceedings of the 61st IEEE International Conference on Communications (**ICC**), 2025.

[3] Wenshu Fan, Hongwei Li, Wenbo Jiang, **Haotian Deng**. "Making Audio Data Unlearnable." In Proceedings of the 61st IEEE International Conference on Communications (**ICC**), 2025.

[4] **Haotian Deng**, Shengli Pan. "Evaluating Network Boolean Tomography under Byzantine Attacks." In Proceedings of the IEEE Global Communications Conference (**GLOBECOM**), 2023.

PROGRAM ANALYSIS & VULNERABILITY RESEARCH

CALLIX — Callsite-Level Access Control Analysis for Android Firmware First author · NDSS'27

Static analysis framework; foundation of my NDSS submission in 2027.

819 vulnerable paths · **1,750** pre-installed apps · **10** top-tier vendors · **94.3%** precision · **175** vendor-confirmed paths

- Introduced the notion of **sensitive callsites**: identify security-critical operations by jointly reasoning about a generic system API's functionality *and* the sensitivity of the data it touches — catching flaws that API-level, sink-based tools miss (only 3 of 232 confirmed true positives were covered by the sink set of FirmScope, the prior state of the art).
- Formalized access control branch conditions into **security properties** and introduced a **restriction context** to decide whether enforced checks are *sufficient*, detecting missing access control, insufficient restrictions, and restrictions based on unreliable information.
- Implemented on **Soot / FlowDroid / LeakScope** with inter-procedural taint analysis and backward slicing, augmented by **LLM-assisted** semantic interpretation under evidence-based constraints.
- Evaluated on 50 firmware images (1,750 apps after deduplication) from the 10 leading Android vendors: **819** flagged vulnerable paths across **424 ContentProviders**, 94.3% precision on a 30% manual sample; **175** vendor-confirmed to date, several rewarded through bug-bounty programs.

Large-Scale Android OEM Vulnerability Disclosure Independent research · Feb 2025 – Present

Reverse engineering + PoC development across five major vendors.

- Authored **140+ vulnerability reports** with working proof-of-concept exploits against pre-installed apps from **Xiaomi, Samsung, OPPO, HONOR, and vivo** — covering exported `ContentProvider` and `Service` components.
- Discovered access control bypasses, permission-bypass data leaks, and privilege escalation enabling, e.g., arbitrary AI Agent command execution (e.g., remote vehicle control, smart-home actuation, and unauthorized personal messaging), obtaining full-set dangerous permissions, read/write arbitrary files (e.g., photos, media videos, and storage files), forging SMS conversations, and unauthorized location access.
- Responsibly disclosed findings; many **confirmed and bug-bounty rewarded** by vendor security programs. This corpus served as real-world ground truth for evaluating CALLIX.

SELECTED RESEARCH PROJECTS

Secure Model Inference on Vertically Partitioned Data (SecInfer) First author · Apr 2024 – Nov 2025

- Designed a secure multi-party computation protocol for efficient, privacy-preserving model inference over vertically

partitioned data; published as first author at IEEE ICC 2025. (code)

Byzantine-Robust Network Tomography (NSFC) First author · Jul 2022 – May 2023

- Modeled and evaluated Byzantine attacks against Boolean network tomography; first-author paper at IEEE GLOBECOM 2023. Built `NBT_ByzAtt_GUI`, a visualization tool for the findings. (code, GUI)

TECHNICAL SKILLS

Program Analysis	Static & dataflow analysis, inter-procedural taint tracking, backward slicing, call-graph construction, control-/data-flow modeling; Soot, FlowDroid
Reverse Engineering	Android app & firmware analysis, DEX/Smali bytecode; jadx, apktool, adb
Security	Android internals & permission model, access control, privilege-escalation analysis, responsible disclosure; secure multi-party computation
Languages	Java, Python, C/C++

OPEN-SOURCE CONTRIBUTION

Moby / Docker Engine — Linux Capabilities Fix via openKylin · 2023

- Found and patched a container-startup flaw (< v20.10.14) where non-empty *inheritable* Linux process capabilities let unprivileged programs raise capabilities into the permitted set. Verified the issue and submitted the fix. (contribution)

EDUCATION

University of Electronic Science and Technology of China (UESTC), Chengdu Sep 2024 – Present
M.S. in Cyberspace Security · *Advisor: Prof. Hongwei Li*

Beijing University of Posts and Telecommunications (BUPT), Beijing Sep 2020 – Jul 2024
B.Eng. in Information Security

LEADERSHIP & SERVICE

Class President, School of Cyberspace Security, BUPT (2020–2024) · Leader, Key Social Practice Program, BUPT (2022) · Intern, China Cybersecurity Association (2022) · Intern, Beijing Softcom Power — openEuler/openGauss database engineering (2023).