Mr. Yunjie Deng

yunjie.deng@gatech.edu LinkedIn Profile Google Scholar

Education

- Aug. 2023 - Present, **Ph.D. in Computer Science**, **Georgia Institute of Technology**
  Advisor: Sukarno Mertoguno
- Aug. 2020 - July 2023, **M.E. in Computer Science**, **Southern University of Science and Technology**
  Advisor: Fengwei Zhang
- Aug. 2016 - July 2020, **B.E. in Computer Science**, **Southern University of Science and Technology**
  Advisor: Xin Yao

Selected Projects

Mole: Breaking GPU TEE with GPU-Embedded MCU (CCS'25)

- We observe the presence of the microcontroller unit (MCU) in modern GPU devices and leverage it to attack GPU computation and the host system. By reverse-engineering the MCU on Arm Mali GPUs, we figure out the firmware workflow and construct malicious mapping in the page table to enable its arbitrary memory-access capabilities. We further prototype an MCU-based attack that exfiltrates and tampers with GPU computation data, even under existing GPU TEE protections, thereby threatening AI models running on the GPU. This work highlights risks in Mali GPU firmware and provides a new attack vector for bypassing the system security mechanism.
- GitHub link: CCS'25 Mole

Strongbox & Cage: Building GPU TEEs on Arm Devices (CCS'22 & NDSS'24 & TDSC'23,25)

- Trusted Execution Environments (TEEs), such as Arm TrustZone and Arm Confidential Compute Architecture (CCA), have been proposed to secure user applications against high-privilege attackers. However, existing TEE techniques focus primarily on protecting CPU-side computations, while overlooking the security of sensitive GPU workloads. To extend TEE protection to GPU computation, we leverage Arm hardware features, including Stage-2 translation, TrustZone, and CCA, to enforce security at the GPU level. We design and implement GPU TEEs that provide memory isolation for both GPU memory and MMIO registers, ensuring secure GPU computation even in the presence of high-privilege attackers.
- GitHub link: CCS'22 Strongbox & NDSS'24 CAGE

BootRIST: Detecting and Isolating Mercurial Cores in CPUs (ESORICS'24)

- Silent CPU computation faults can compromise user data without producing any obvious error indications, causing errors to propagate and affect a wider range of data. To address this problem, we design and implement an OS-level framework on AArch64 Linux to detect silent CPU faults during the boot stage. The framework operates during Linux kernel initialization and employs instruction fuzzing to test fault-prone CPU cores. A voting-based algorithm is then applied to identify faulty cores, which are subsequently isolated by Linux CPU management mechanisms to ensure overall system reliability.

Publications

(means equal contribution)*

- Hongyi Lu*, **Yunjie Deng***, Sukarno Mertoguno, Shuai Wang, and Fengwei Zhang. "Mole: Breaking GPU TEE with GPU-Embedded MCU." In Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security. 2025. [**CCS'25**]
- **Yunjie Deng**, Chenxu Wang, Shunchang Yu, Shiqing Liu, Zhenyu Ning, Kevin Leach, Jin Li et al. "Strongbox: A gpu tee on arm endpoints." In Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security, pp. 769-783. 2022. [**CCS'22**]
- Chenxu Wang*, **Yunjie Deng***, Zhenyu Ning, Kevin Leach, Jin Li, Shoumeng Yan, Zhengyu He, Jiannong Cao, and Fengwei Zhang. "Building a lightweight trusted execution environment for arm gpus." IEEE Transactions on Dependable and Secure Computing 21, no. 4 (2023): 3801-3816. [**TDSC'23**]
- Yihao Luo*, **Yunjie Deng***, Jingquan Ge, Zhenyu Ning, and Fengwei Zhang. "BootRIST: Detecting and Isolating Mercurial Cores at the Booting Stage." In European Symposium on Research in Computer Security, pp. 85-103. Cham: Springer Nature Switzerland, 2024. [**ESORICS'24**]

- Chenxu Wang, Fengwei Zhang, **Yunjie Deng**, Kevin Leach, Jiannong Cao, Zhenyu Ning, Shoumeng Yan, and Zhengyu He. "Cage: Complementing arm cca with gpu extensions." In Network and Distributed System Security (NDSS) Symposium, vol. 2024. 2024. **[NDSS'24]**
- Chenxu Wang, Kun Lu, Fengwei Zhang, **Yunjie Deng**, Kevin Leach, Jiannong Cao, Zhenyu Ning, Shoumeng Yan, Tao Wei, and Zhengyu He. "Building Confidential Accelerator Computing Environment for Arm CCA." IEEE Transactions on Dependable and Secure Computing (2025). **[TDSC'25]**
- Fengwei Zhang, Chenxu Wang, **Yunjie Deng**, Shoumeng Yan, and Zhengyu He. "Methods and apparatuses for executing gpu task in confidential compute architecture." U.S. Patent Application 18/980,904, filed June 19, 2025.
- Muhammad Faraz Karim, **Yunjie Deng**, Luyao Niu, Bhaskar Ramasubramanian, Michail Alexiou, Dinuka Sahabandu, Radha Poovendran, and Sukarno Mertoguno. "Rapid Autonomy Transfer in Reinforcement Learning with a Single Pre-Trained Critic." In 2024 IEEE 36th International Conference on Tools with Artificial Intelligence (ICTAI), pp. 1000-1007. IEEE, 2024. **[ICTAI'24]**
- Er Zhuo*, **Yunjie Deng***, Zhewei Su, Peng Yang, Bo Yuan, and Xin Yao. "An experimental study of large-scale capacitated vehicle routing problems." In 2019 IEEE Congress on Evolutionary Computation (CEC), pp. 1195-1202. IEEE, 2019. **[CEC'19]**

Experience

June 2019 - Aug. 2019, Tencent (Shenzhen, China), Software Engineer Internship (Windows development)

Skills & Tools

- **Programming Languages:** C/C++, Python, Java, OpenCL, cuda, rust, pytorch
- **Tools:** Intel PIN, DynamoRIO, GDB, angr, IDA Pro, eBPF, LLVM
- **Development Platforms:** Linux kernel development, AArch64 development, Arm TrustZone, Arm Trusted Firmware, Embedded Systems