Yunjie Deng

🌐 Yunjie Deng's Page
✉ dengyj2020@mail.sustech.edu.cn

🎓 Education

Southern University of Science and Technology (SUSTech), China — 2020 – Present
M.E. in Computer Science and Engineering, GPA 3.65/4.00 (ranked 3/71) — *Shenzhen, Guangdong*

Southern University of Science and Technology (SUSTech), China — 2016 – 2020
B.E. in Computer Science and Engineering, GPA 3.84/4.00 (ranked 4/158) — *Shenzhen, Guangdong*

🌐 Publications

> **StrongBox: A GPU TEE on Arm Endpoints.**
> Yunjie Deng, Chenxu Wang, Shunchang Yu, Shiqing Liu, Zhenyu Ning, Kevin Leach, Jin Li, Shoumeng Yan, Zhengyu He, Jiannong Cao, Fengwei Zhang
> In *Proceedings of the 29th ACM Conference on Computer and Communications Security (CCS'22)*

> **An Experimental Study of Large-scale Capacitated Vehicle Routing Problems**
> Er Zhuo, Yunjie Deng, Zhewei Su, Peng Yang, Bo Yuan, Xin Yao
> In *2019 IEEE Congress on Evolutionary Computation (CEC 2019)*

🌐 Research Experience

StrongBox: A GPU TEE on Arm Endpoints — Sep. 2020 – May 2022
Mentors: Fengwei Zhang, Zhenyu Ning

> We design and implement StrongBox, the first Arm endpoint GPU Trusted Execution Environment (TEE). Based on the shared memory architecture of endpoints GPU and the existing Arm hardware features, we guarantee the security of GPU computation with minimal TCB and high compatibility. StrongBox builds a secure data path between untrusted OS and GPU, allowing GPU to process the data securely. During sensitive GPU computation, StrongBox dynamically manages the access permission of both GPU MMIO register and GPU memory to provide an exclusive execution environment and ensure data confidentiality.

Mercurial Core Detection and Isolation — Oct. 2021 – Present
Mentors: Fengwei Zhang, Zhenyu Ning, Jingquan Ge

> Mercurial core is one type of processor core failure that returns silent corruption computation results occasionally and has been discovered in modern commercial systems. To mitigate the risk of mercurial cores, we design a mercurial core detection framework to detect the potential mercurial cores and isolate them during the operating system kernel booting process.

Compression and Deployment of Deep Neural Network Model on Endpoint Device — Sep. 2019 – Jun. 2019
Mentors: Xin Yao, Peng Yang

> Some deep neural network models require to be deployed on endpoint devices to reduce network communication overhead and provide stable response time. However, due to the limited hardware resource, it is challenging to directly deploy the heavy deep neural network model on endpoint devices. Therefore, this project employs the deep neural network compression algorithm to reduce the parameter size of the deep neural network model while maintaining high inference accuracy.

2-Echelon Location-Routing Problem — Mar. 2019 – Jul. 2019
Mentors: Xin Yao, Peng Yang

> 2-Echelon Location-Routing Problem is an NP-hard problem. We employ the evolutionary algorithm to solve the problem and obtain an acceptable solution within a relatively short time.

An Experimental Study of Large-scale Capacitated Vehicle Routing Problems   Sep. 2018 – Jan. 2019

Mentors: Xin Yao, Peng Yang

> The previously proposed Scalable Approach Based on Hierarchical Decomposition (SAHiD) has shown its superiority on large-scale capacitated arc routing problems (CARP) in terms of both computational efficiency and solution quality. Motivated by the observations of the similarity between CARP and Capacitated Vehicle Routing Problem (CVRP), we employ the SAHiD algorithm on CVRPs and analyze the algorithm performance.

🔖 Honors

SUSTech Excellent Graduated Student of the Department of Computer Science and Engineering   2020

SUSTech Excellent Graduated Student of the ShuLi College   2020

SUSTech Undergraduate Excellent Scholarship of the ShuLi College   2017, 2018, 2019

SUSTech Excellent Freshman Scholarship   2016