1615 Greenfield Ave. Apt. 15
Los Angeles, CA 90025
richard97@g.ucla.edu

Botong Ou

(310) 622-2954
github.com/oubotong

Projects

Cluster Computing on Edge **UCLA NESL LAB** **Fall 2020 – Spring 2021**

- We provide the first framework to support deploying applications across sensors and actuators.
- We also design a corresponding resource manager and deploy it on the IoT network.
- A new layer of abstraction is deployed in conjunction with classical Docker container orchestration.
- This work is submitted to OSDI 2021.
- All the papers below are still under review, I can provide temporary links for them if needed.
- Link: https://github.com/oubotong/edge-rm
- Utilized: Python, Docker, Zephyr, JavaScript, Webassembly

WASI-SN: **UCLA NESL LAB** **Summer 2020 – Fall 2020**

- Extend WebAssembly interface within the context of sensor network.
- Provide several generic platform-agnostic sensor interfaces in Webassembly runtime.
- Build the first Webassembly based MQTT-SN library with WKD-IBE encryption scheme.
- The framework we build achieve 2% additional overhead compared to the native application without sandboxing.
- Link: https://github.com/oubotong/WASI-SN
- Submitted to IOTDI 2021
- Utilized: C, WebAssembly, MQTT-SN, OpenThread, Zephyr

Edge Secure DL framework **UCLA NESL LAB** **Fall 2019 - Spring 2020**

- Built a secure framework on ARM with the help of TrustZone for secure inference.
- Utilize the ARM-NN neural network acceleration library to reduce the latency and memory consumption.
- The neural network is loaded in the unsecure region, but all the calculations are computed in TrustZone.
- Prevent the attacker from compromise the embedded OS to get the data and inference result.
- Link: https://github.com/oubotong/arm-secure-nn
- Submitted to IOTDI 2021
- Utilized: C, ARM-NN, LLVM, Yolo, Cifar, TrustZone

TinySecontainer **Ohio State University** **Summer 2018 – Spring 2019**

- Designed a fine-grained security policy distributor for Docker container.
- Create a new Docker engine for distributing different security policy to different threads inside the container.
- Container now does not rely on a global security policy configuration like Seccomp, user can set up different policies for the processes inside the same container.
- Link: https://github.com/oubotong/TinySecontainer
- Utilized: Golang, Docker, Seccomp, BPF, XML, PIN

LLVM obfuscator **Shanghai Jiaotong University** **Spring 2018 – Summer 2018**

- Design a program obfuscator based on LLVM for fuzzing program written in C, C++ and Rust to improve the robustness and increase the difficulty for reverse engineering.
- Introduce three methods: string encryption, control flow flattening and instruction substitution.
- The obfuscated program only have 10% more bytecode compared to the original binary.
- Link: https://github.com/oubotong/Armariris
- Utilized: C, C++, Rust, LLVM, AES-256, IDA Pro

Education

Los Angeles, CA **University of California, Los Angeles** **Fall 2019 – Now**

- Pursuing Ph.D. degree in Computer Science; GPA: 3.84/4.0
- Mentor: Mani Srivastava
- Coursework: Machine Learning Algorithms; Network Algorithms; Advanced Database; Current Topic of Data Analysis, Intelligent IoT system, Adversarial Machine Learning, Named Data Network, Network Verification

Shanghai, China **Shanghai Jiaotong Universirty** **Fall 2015 – Summer 2019**

- B.S. degree in Computer Science; GPA: 3.7/4.0
- Coursework: Operating System; Computer Architecture; Computer Network; Introduction to Cryptology and Information Security; Algorithm and Complexity…

Languages and Technologies

- C++, C, Python, Golang, JAVA, WebAssembly, Wasm-Runtime
- OpenThread, Docker, IoT, Embedded System, Kubernetes, Caffe, Eclipse, PIN, Zephyr