CHI-SHENG CHEN

Embedded System Developer

Phone: +886-979-931-001
Email: johnny1001s000602@gmail.com
GitHub: rota1001

Education

National Cheng Kung University (Sep 2023 – Jun 2027)

- B.S. in Computer Science and Engineering
- Academic Excellence Award (**Top 5%** for 3 semesters)
- Relevant Coursework: Operating System, Linux Kernel Design, Algorithms, Data Structures

Competitions

Programming Contests

- 2025 ICPC Taichung Regional — Bronze Medal
- 2025 Asia Taiwan Online Programming Contest — Silver Medal
- 2024 ICPC Taichung Regional — Bronze Medal
- 2024 National Collegiate Programming Contest — 4th Place Award
- 2024 Asia Taiwan Online Programming Contest — Silver Medal

CTF Contests (Security)

- HITCON CTF 2025 Quals — Ranked 2nd (Taiwan) / Ranked 22nd (Global), write-up[1]
- Crypto CTF 2025 — Ranked 38th (Solo, Global), write-up[2]

Side Projects

Bare-metal Operating System for STM32F103

Description: A preemptive multitasking OS running on STM32F103 without the STM32 HAL.

Links: Github[3] Hackmd[4]

- Reduced instruction fetch latency by executing the kernel entirely in SRAM
- Implemented **privilege separation** between kernel and user tasks
- Built a **preemptive scheduler** supporting round-robin scheduling and **cooperative yielding**
- Implemented context switch using **setjmp/longjmp**
- Designed syscall mechanism scheduled as kernel tasks instead of running in handler mode
- Implemented UART with **memory-mapped I/O**

Linux Kernel Instrumentation Framework (HITCON 2025)

Description: Kernel module for dynamic instrumentation capable of intercepting kernel execution paths **without kallsyms or kprobes**. Presented at *HITCON 2025*.

Links: Github[5] Hackmd[6]

- Inspected and modified **procfs** file operations by parsing its internal tree structure
- Resolved syscall function addresses by analyzing the **syscall handler** in the Linux kernel (without relying on exported syscall table)
- Performed runtime kernel patching via **PTE flag manipulation**
- Achieved process concealment by manipulating the internal **PID hash** structure used by the scheduler
- Patched the **ELF header and entry point** to embed a minimal payload that invokes the kernel's module-loading syscall during systemd startup

Microcomputer with Custom OS and Peripheral Integration

Description: Built a microcomputer using PIC18F microcontroller integrating keyboard, SRAM, UART, and USB storage.

Links: Github[7] Hackmd[8]

- Developed **USB Host driver** for CH375 supporting **HID keyboard** and USB flash drive
- Built external memory interface enabling **1-byte-per-instruction** block access using **only an 8-bit GPIO** with latch/counter/D-trigger, using a **logic analyzer** to debug hardware timing
- Implemented **DMA mechanism** using 512KB SRAM as disk cache

Presentation

- HITCON 2025 — *A Kernel Rootkit That Works Without Kallsyms*[9]

Links

[1] https://hackmd.io/@rota1001/hitcon-ctf-quals-2025

[2] https://hackmd.io/@rota1001/crypto-ctf-2025

[3] https://github.com/rota1001/arm-os-101

[4] https://hackmd.io/@rota1001/stm32-os

[5] https://github.com/rota1001/ksymless

[6] https://hackmd.io/@sysprog/r1l3i4_Zge

[7] https://github.com/beautiful-fruit/picos

[8] https://hackmd.io/@weiso131/picos

[9] https://hitcon.org/2025/en-US/agenda/f679c826-4c37-4989-bf27-6e44ea4726ce/