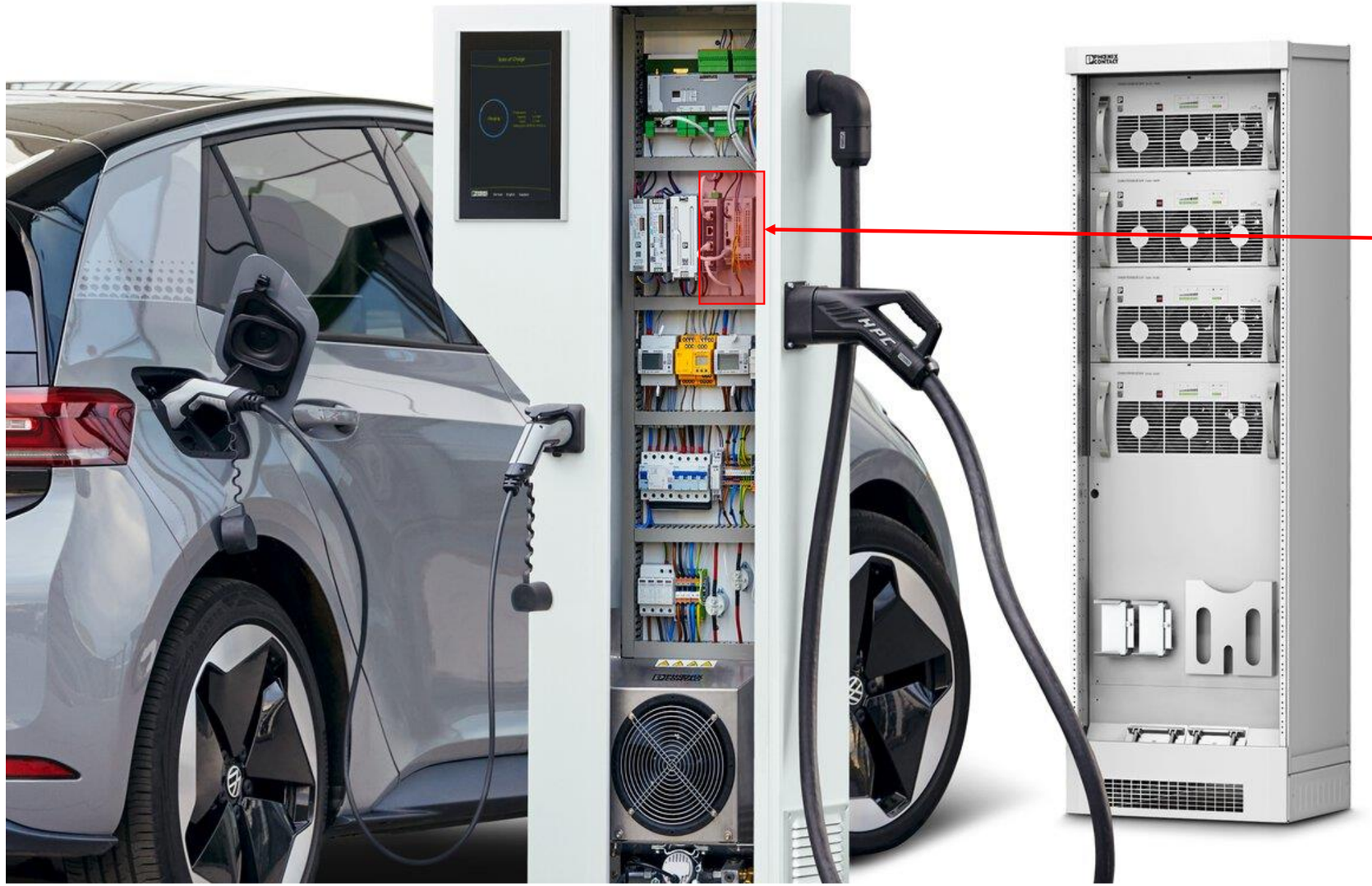
Hands-on Firmware Extraction, Exploration, and Emulation

Quentin Kaiser (quentin.kaiser@onekey.com)

Today's Target



Electric Vehicle Charging Station Controller

CHARX control modular, AC charging controller, with Embedded Linux system, IEC 61851-1, operating mode: Stand-Alone, Client, Server,

Interfaces:
- Ethernet (2x)
- Cellular communication (4G/2G)
- CHARX control modular system bus
- MICRO-USB type C

Communication protocols:
- OCPP 1.6J
- Modbus/TCP
- MQTT

Connectable peripheral devices:
- Energy meter
- RFID
- DC residual current detection
- DIN rail mounting

Today's Target

Electric Vehicle Charging Station Controller

CHARX control modular, AC charging controller, with Embedded Linux system, IEC 61851-1, operating mode: Stand-Alone, Client, Server,

Interfaces:
- Ethernet (2x)
- Cellular communication (4G/2G)
- CHARX control modular system bus
- MICRO-USB type C

Communication protocols:
- OCPP 1.6J
- Modbus/TCP
- MQTT

Connectable peripheral devices:
- Energy meter
- RFID
- DC residual current detection
- DIN rail mounting

Electric Vehicle Chargers Category

There's been a fair amount of research into the security of EVs, but there hasn't been as much scrutiny around what we plug into an EV. Attack surfaces such as mobile apps, Bluetooth Low Energy (BLE) connections, and the OCPP protocol could all allow threat actor to cause harm to an EV. For this event, we'll have six different EV Chargers available as targets. An attempt in this category must be launched against the target's exposed services or against the target's communication protocols/physical interfaces that are accessible to a typical user.

Target	Cash Prize	Master of Pwn Points
ChargePoint Home Flex	$60,000	6
Phoenix Contact CHARX SEC-3100	$60,000	6
EMPORIA EV Charger Level 2	$60,000	6
JuiceBox 40 Smart EV Charging Station with WiFi	$60,000	6
Autel MaxiCharger (MAXI US AC W12-L-4G)	$60,000	6
Ubiquiti Connect EV Station	$60,000	6

Today's Plan

Extraction

Extract the controller firmware with unblob.

Two firmwares: official update from manufacturer, and memory dump from live device.

Exploration

Finding relevant items to build the right kernel and create the proper interfaces.

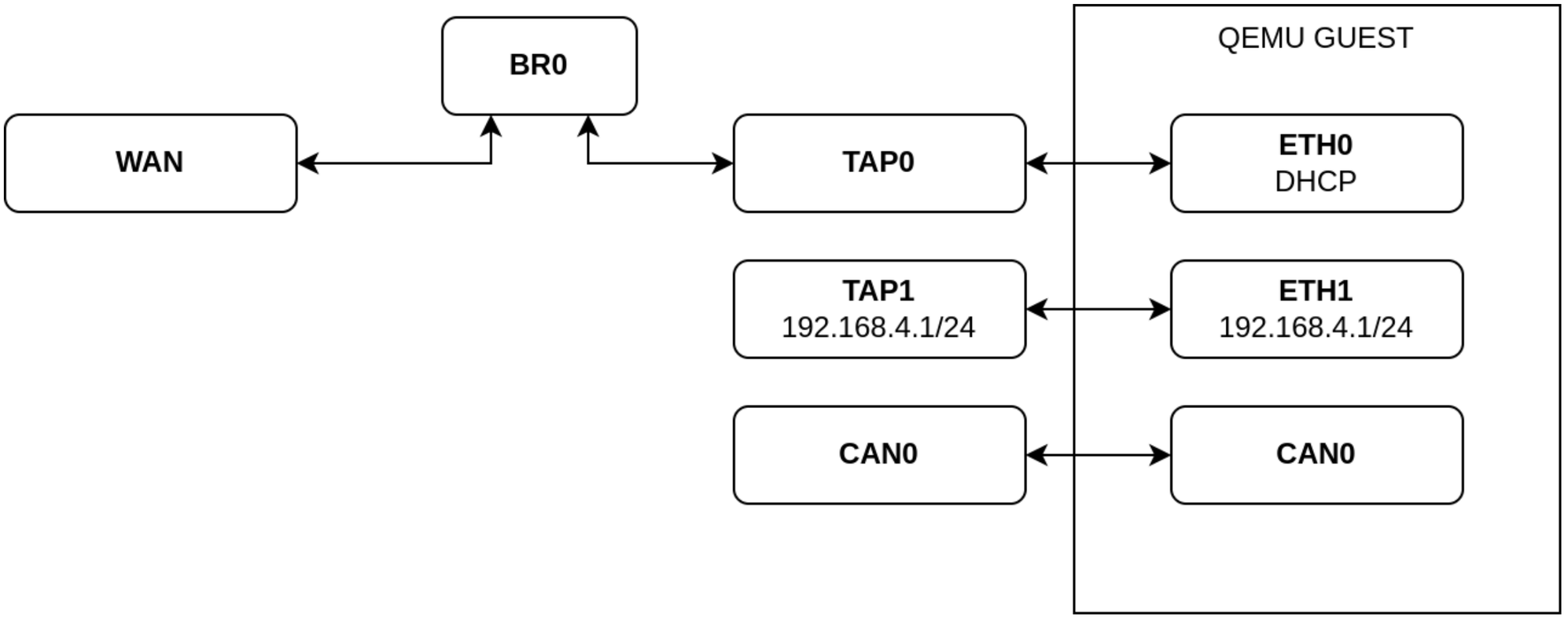
Emulation

Full system emulation with QEMU using the extracted firmware.

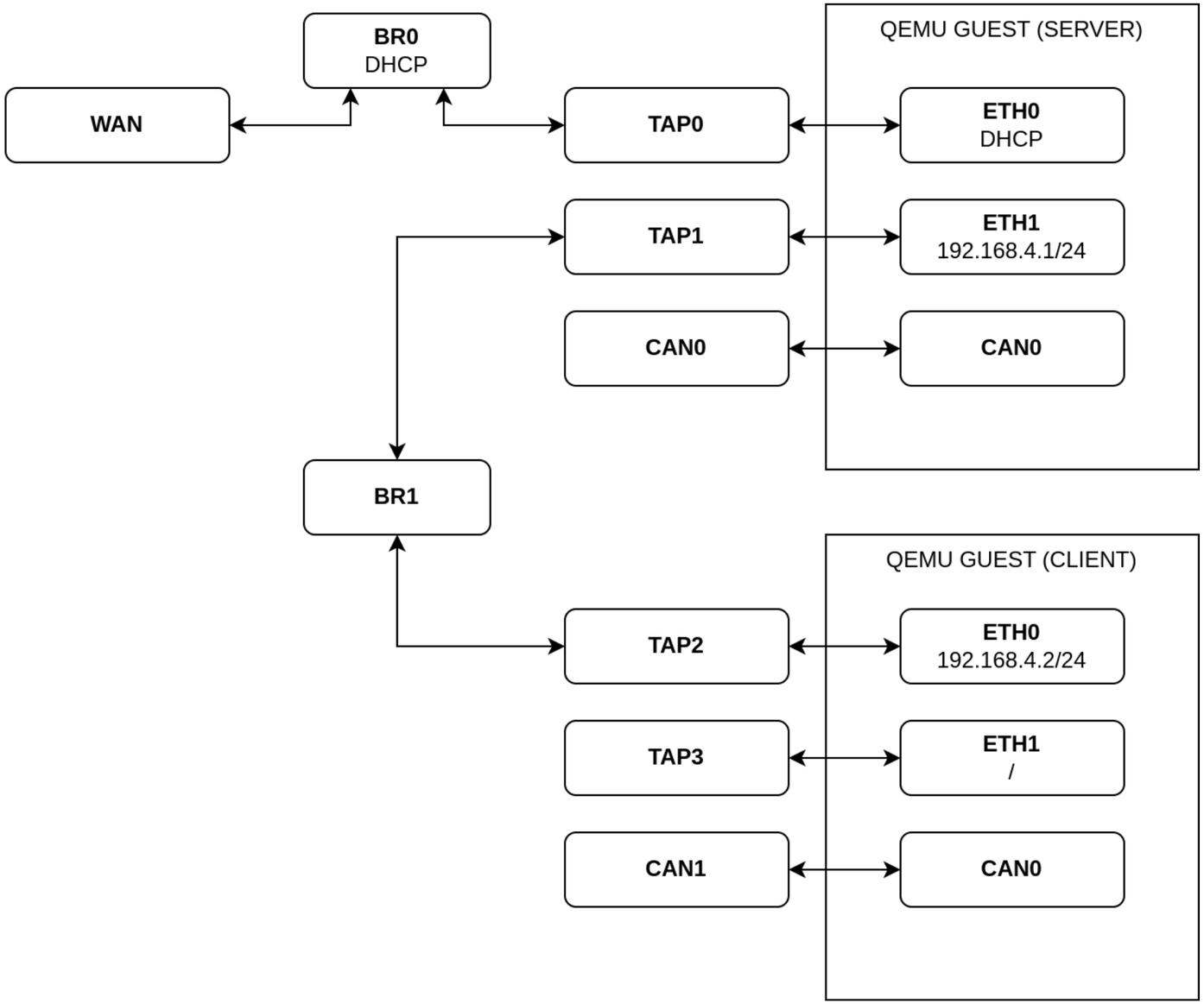
Information Gathering

- Platform: **Phytec phyBOARD-Segin i.MX6 UltraLite**
- Architecture: **ARMv6**
- CPU: **Cortex-A7**
- Bootloader: ?
- OS: **Linux version 4.14.93**
- Peripherals:
  - **2 Ethernet** interfaces
  - **1 CANbus** interface
  - **USB / USB OTG**

Ethernet & CANBUS Networking



Ethernet & CANBUS Networking



Thank you !