Hack In The Box

开源硬件在安全研究中的应用

Applications of Open Source Hardware in Security Research

GeWu Lab @Nsfocus
Maliang

NSFOCUS

About Me

- Maliang
- Nsfocus　GeWu Lab
- Over 10 years of experience in embedded development in the IoT, telecom and industrial control systems.
- Now a security researcher on industrial IoT security at NSFOCUS.

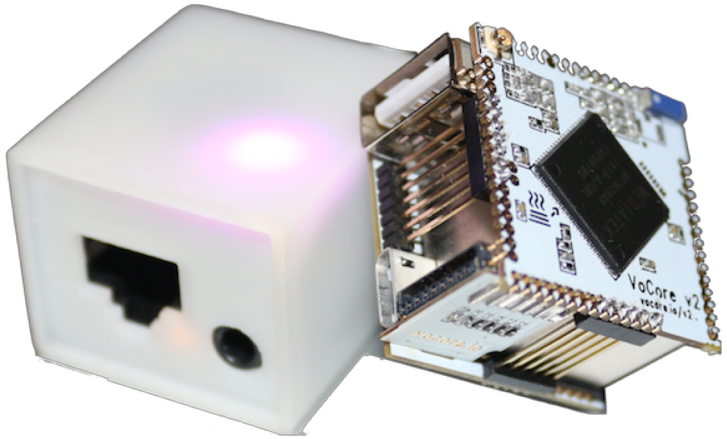
NSFOCUS

目录
CONTENTS

NSFOCUS

Overview

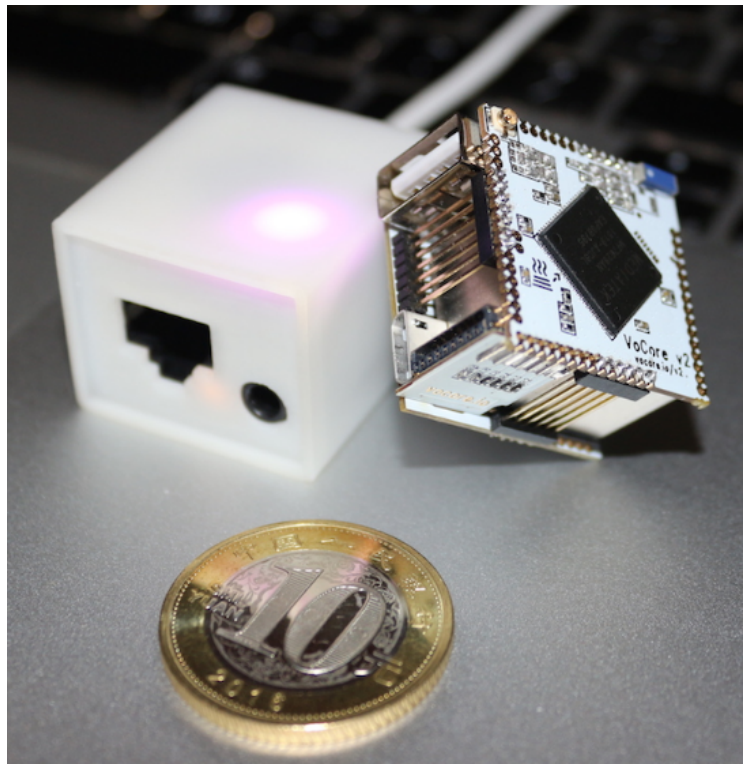
- Introducing a fun open source hardware: VoCore2
- Introduce embedded Linux build process
- Introduce the build process of OpenWRT



- Introduce three application scenarios of VoCore2 in security.
- I hope everyone will have fun from open source hardware projects.

Introduction to VoCore2

- VoCore2is a crowdfunding project (open source)
- http://vocore.io/v2u.html
- Priced at $11.99 (¥250)
- CPU : 580 MHz, MIPS
- RAM : 128MB
- FLASH : 16MB
- 300Mbps Wi-Fi
- Ethernet interface
- USB 2.0 port
- Micro SD slot
- audio port
- GPIO



NSFOCUS

Overview

- VoCore2 is open hardware and runs OpenWrt.
- It has WIFI, USB, UART, 20+ GPIOs but is only one inch square.
- You will not only get the VoCore2 but also its full hardware design including schematic, circuit board, bill of materials; full source code (including boot loader), operating system (openwrt) and applications.
- It will help you to make a smart house, study Pwn, study embedded system or even make the tiniest router in the world.

目录
CONTENTS

NSFOCUS

Construction of embedded Linux system

- Create a Linux cross-compilation environment
- Create a bootloader
- Porting the Linux kernel
- Create Rootfs (root file system)
- Write and install drivers
- Write and install software
- Firmware package

Open source hardware overview

Construction of embedded Linux system

Construction of OpenWRT system

Several typical applications of VoCore2 in security

NSFOCUS

Introduction to OpenWRT

- The OpenWrt Project is a Linux operating system targeting embedded devices.
- Instead of trying to create a single, static firmware, OpenWrt provides a fully writable filesystem with package management.
- This frees you from the application selection and configuration provided by the vendor and allows you to customize the device through the use of packages to suit any application.
- For developers, OpenWrt is the framework to build an application without having to build a complete firmware around it;
- for users this means the ability for full customization, to use the device in ways never envisioned.

OpenWRT is highly integrated

- Cross compilation tool
- Linux kernel
- BusyBox
- File system
- Firmware driver
- Most used software
- Interface plugin
- …

VoCore2 and security-related compilation options

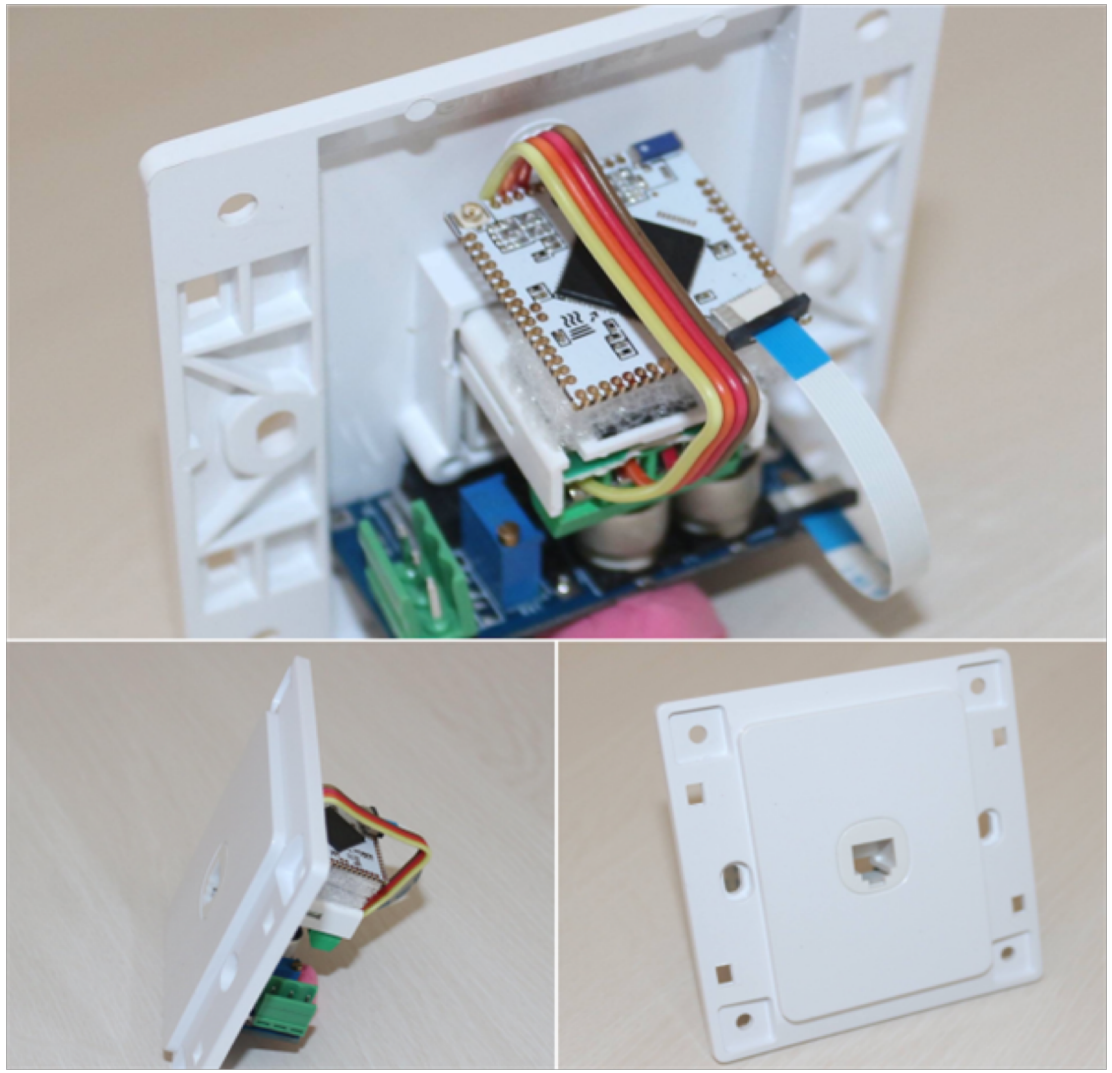
目录
CONTENTS

NSFOCUS

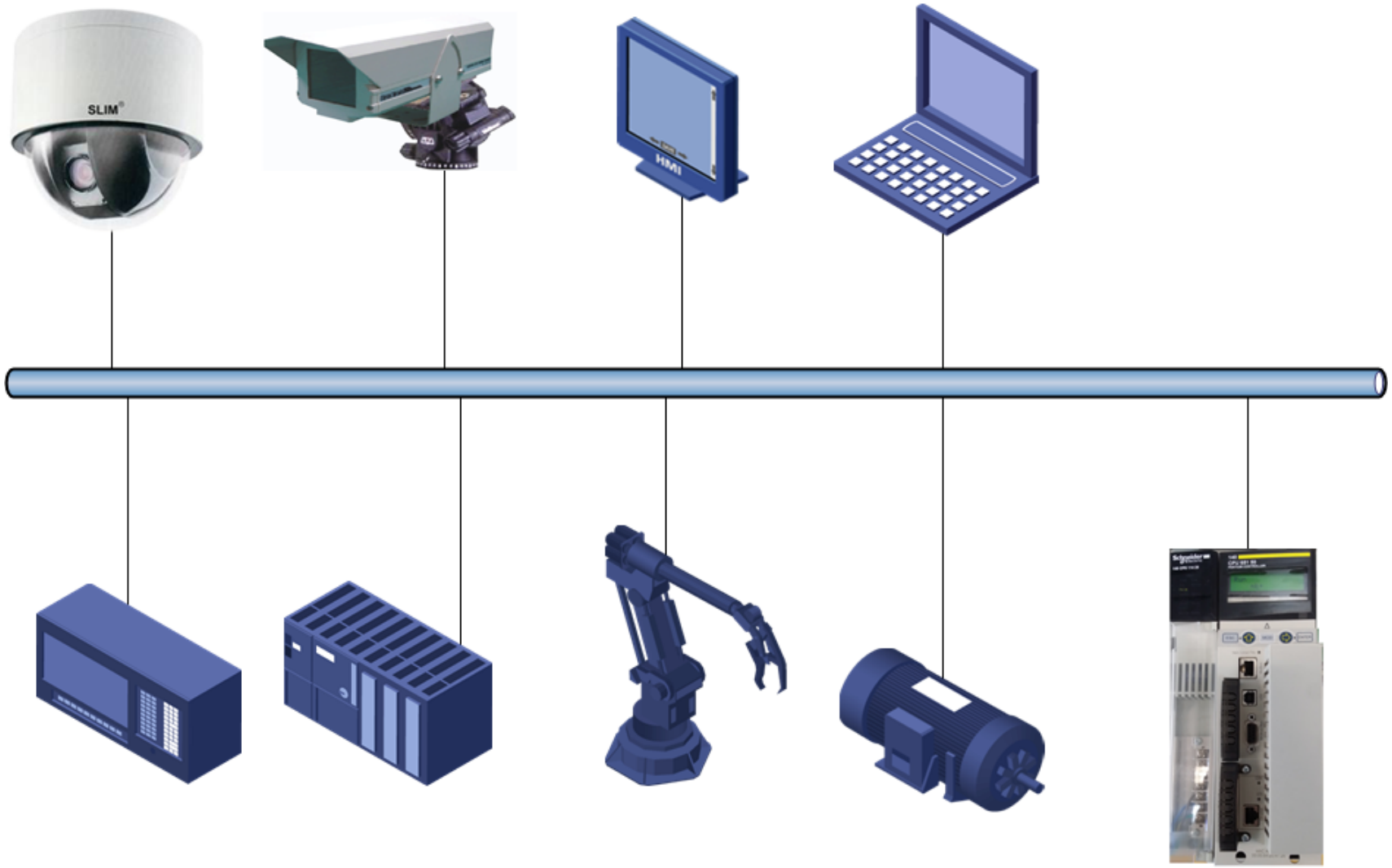
Trial environment for DIY vulnerability debugging

- VoCore2 is a system built by MIPS architecture
- At compile time, you can choose various debugging tools such as python, GDB, nc, etc.
- Can debug various MIPS vulnerabilities
- Used to practice Pwn topics

DIY hidden camera

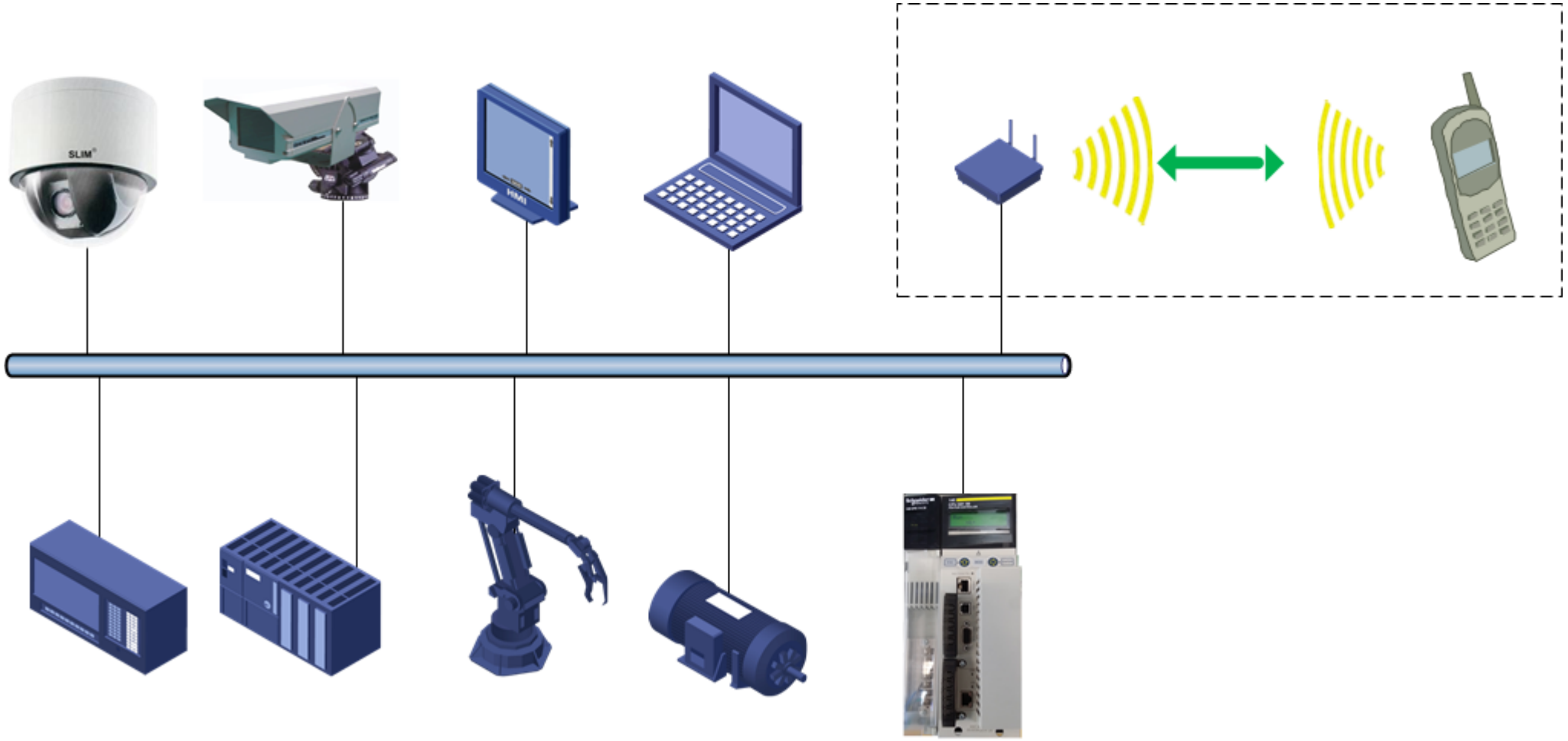


Remote wireless penetration spy device case in industrial environment



NSFOCUS

Remote wireless penetration spy device case in industrial environment



Remote wireless penetration spy device in industrial control environment

- Placing a clipped video

Thank You !

NSFOCUS