Wireless Hacking with 'HackCUBE'

Yunding Jian, Jie Fu, Chaoran Wang

UnicornTeam, 360 Technology
April 1, 2018
What’s the HackCUBE?

- HackCUBE is a hardware testing platform
- HackCUBE is a so opened platform
- HackCUBE is a well-designed and good-looking platform
The HackCUBE
Core Board of HackCUBE

- Raspberry Pi Zero W
- USB2514B 4*USB HUB
- RTL8822BU 2.4G/5.8G WIFI
- DS1307 RTC
- SPI Flash
- Beep
- MIC
RGB LED Board

- 8*8 RGB LED
- Show Light
- Show Logo
- Flashlight
Power Board

- TI BQ25895
  - Supports Max Charge (QC3.0)
- TI TPS61088
  - Boost to 5V
GPIO Board

- ALL GPIO Extended
Arduino Board

- Arduino Micro Pro 3.3V
- CC1101 433MHz
- CC1101 315MHz
- nRF24L01+ PA
NFC & Anttan Board

- PN532
- EM4095
Connect Board

- 2*25P 0.8mm BTB Connector
- 6*Connector
What can we do: WIFI / BLE

- WIFI Router
- WIFI Advertising
- WIFI Blocking Attack
- WIFI Fishing
- WIFI IOT Gateway
- WIFI ...

- Bluetooth Advertising
- Bluetooth Keyboard/Mouse
- Bluetooth IOT Gateway
- Bluetooth ...

Diagram:

- Raspberry Pi Zero W
  - BCM43438
    - 2.4 GHz 802.11 b/g/n
    - Bluetooth 4.1 + HS Low-energy (BLE)
  - RTL8822BU
    - 2.4G/5GHz 802.11 a/b/g/n/ac
    - Bluetooth V4.1+HS, BLE and be backwards compatible with Bluetooth 1.2, 2.X+ enhance data rate
Demo 1: Wifi Attack

- WIFI AP: HackCUBE_xx:xx:xx
- WIFI Password: hackcube123
- Web Address: 192.168.2.3
- SSH User: root
- SSH Password: hackcube
What can we do: RF

- IOT Sub-1GHz RF Board
- RFCat
- HID Attack Tool
- Remote Control Tool
- Wireless Keyboard
- RF Transmit Mode
Demo 2: RF Control Car
Demo 3: RF Control Quadcopter
Demo 4: Wireless Keyboard

- Keyboard
- USB Network Card
- USB Disk
- BadUSB
What can we do: NFC

- 125KHz NFC Read/Write/Simulation
- Passive Keyless Enter
- 13.56MHz NFC Read/Write
- Crack Mifare Card
**Demo 5: NFC Read/Write**

**Cube NFC Manage Safety Risk Detection for Cards Working at 125Khz, 13.5Mhz.**

<table>
<thead>
<tr>
<th>Read</th>
<th>VID</th>
<th>ID</th>
<th>WRITE</th>
<th>SIMULATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>050</td>
<td>6835882</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Write**

<table>
<thead>
<tr>
<th>VID</th>
<th>ID</th>
<th>WRITE</th>
<th>SIMULATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Simulate**

<table>
<thead>
<tr>
<th>VID</th>
<th>ID</th>
<th>WRITE</th>
<th>SIMULATE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

```bash
nfc-list uses libnfc 1.7.1
NFC device: pn532_spi/dev/spidev0.0 opened
1 ISO14443A passive target(s) found:
ISO/IEC 14443A (106 kbps) target:
ATQA (SENS_RES): 00 04
UID (NFCID1): 0a 1a cd 09
SAK (SEL_RES): 08
```
Our Plan: SDR
Our Plan: Debugger Tool

- OpenJTAG
- Buspirate
- CC Debugger
- Logic Analyzer
- IR Analyzer
- CAN Bus Analyzer
- Zigbee Sniffer
- BLE Sniffer
- Other …
Next: HackCUBE Mini

- Small
- Portable
- High Integration
- Low Price
- Other …
Next: HackCUBE Mini

- Small
- Portable
- High Integration
- Low Price
- Other …
Next: HackCUBE Mini

- Small
- Portable
- High Integration
- Low Price
- Other …
How to get it?

https://github.com/UnicornTeam/hackcube.git

Only limited units for USD299

The official release will be USD399

Option 0: Price are without USD50 shipping cost. World wide.

Option 1: Pay now and collect at #HITB2018SG USD299 NETT
Thank You ~