只要一張小朋友：
利用樹莓派打造物聯網攻擊工具

—— HackMaster Pi

📌 1Ping Sun

在開始之前

本專案及今禁止用於任何違法行

請務必在合。

依據刑法第入侵他人系統、竊取資面臨刑事責任。

技術能力越應用今日所分享的知

目錄

關於我

- 臺北市數位實驗高中高二
- ……

關於 HackMaster Pi

- 以低成本學習物聯網的攻擊與防禦
- 包含藍牙、Wi-Fi、紅外線、RFID、USB 等相關工具
- 使用 Raspberry Pi Zero 2 W

成品照片

關於 HackMaster Pi

	HackMaster Pi	CapibaraZero	Flipper Zero
運算速度	1 GHz	160 Mhz	64 MHz
價錢	$15	$9.99	$169
藍芽	$0	$0	$0
Wi-Fi	$0	$0	$29
紅外線	$3	$3	$0
125 KHz RFID	$2	$2	$0
13.56 MHz RFID	$9	$9	$0
SubGHz	$9	$9	$0
總計	$38	$32.99	$198


功能展示

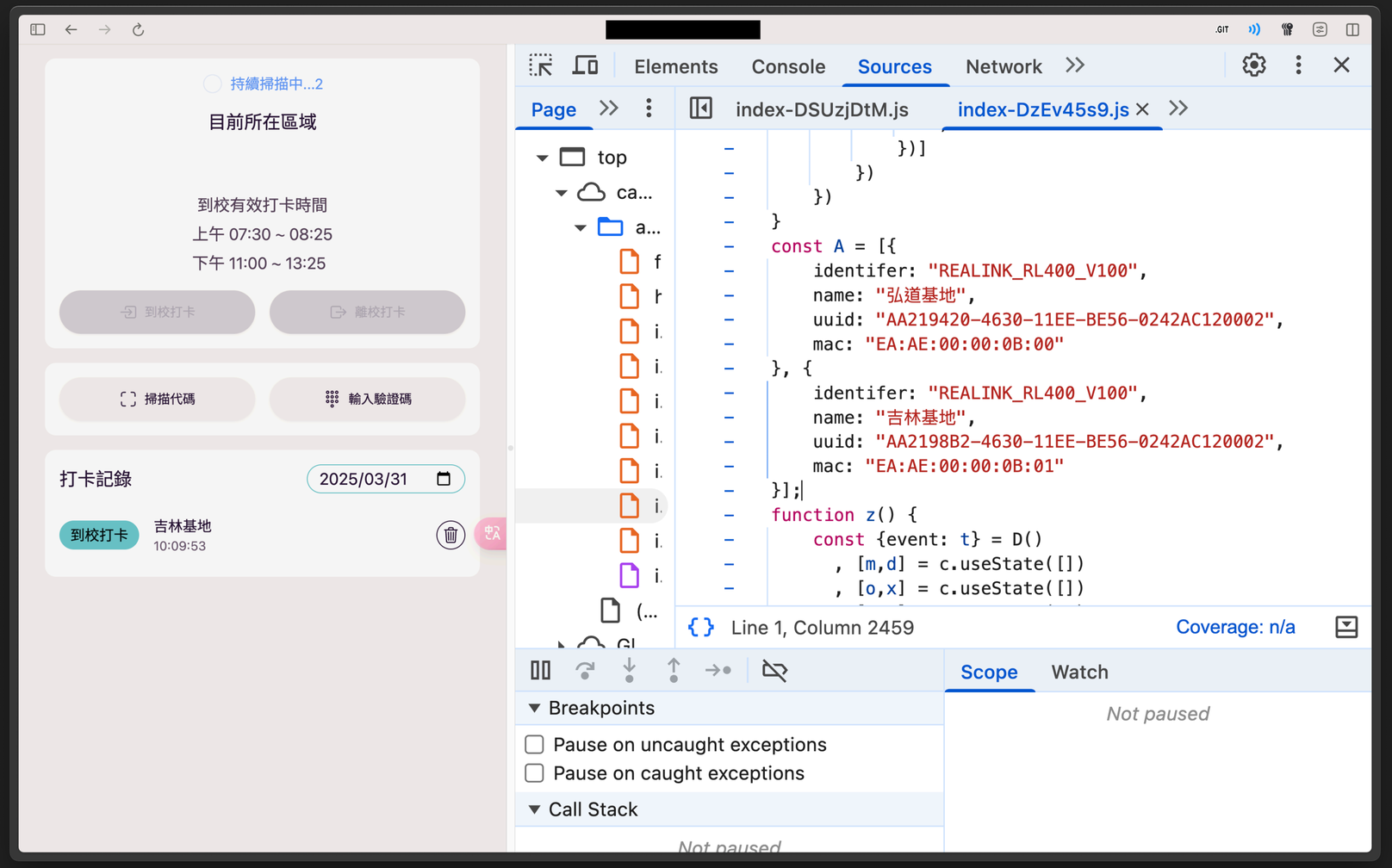
Fake Airpods

圖片來源：https://support.apple.com/zh-tw/104989

BLE Beacon Emulate

BLE Beacon Emulate

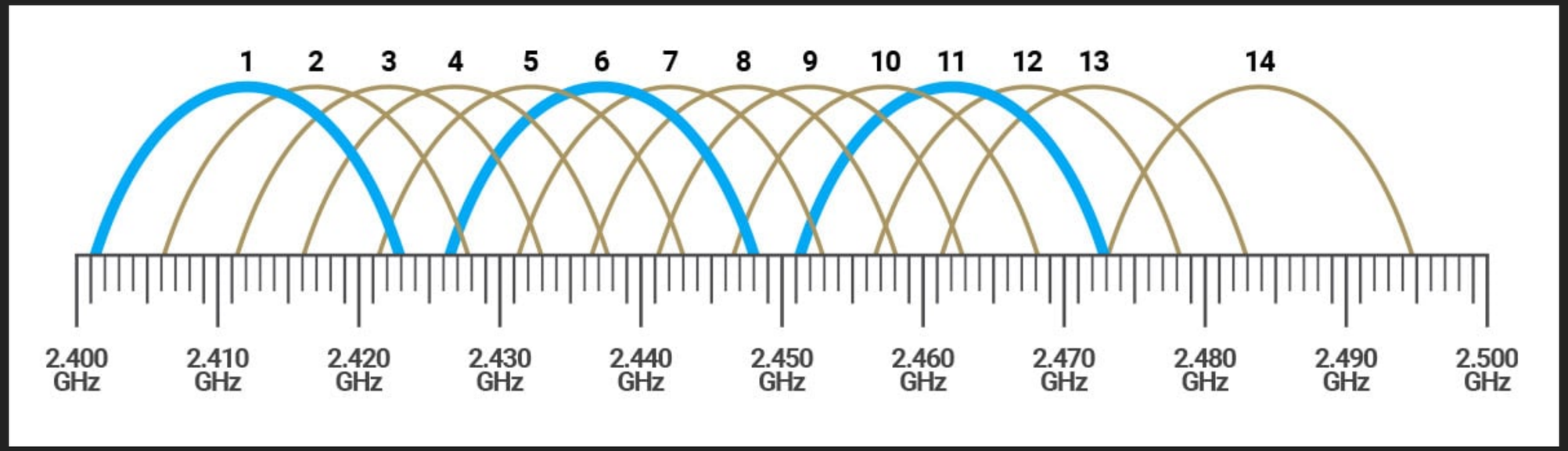
BLE Beacon Emulate



Rickroll Wi-Fi

- // 操作步驟

Rickroll Wi-Fi



圖片來源：https://wattbrother.com/276521

Rickroll Wi-Fi

示例封包（16進位表示）

假設 SSID 為 "Never Gonna"，頻道為 1，隨機 MAC 為 `12:34:56:78:9a:bc`，封包可能如下（簡化版）：

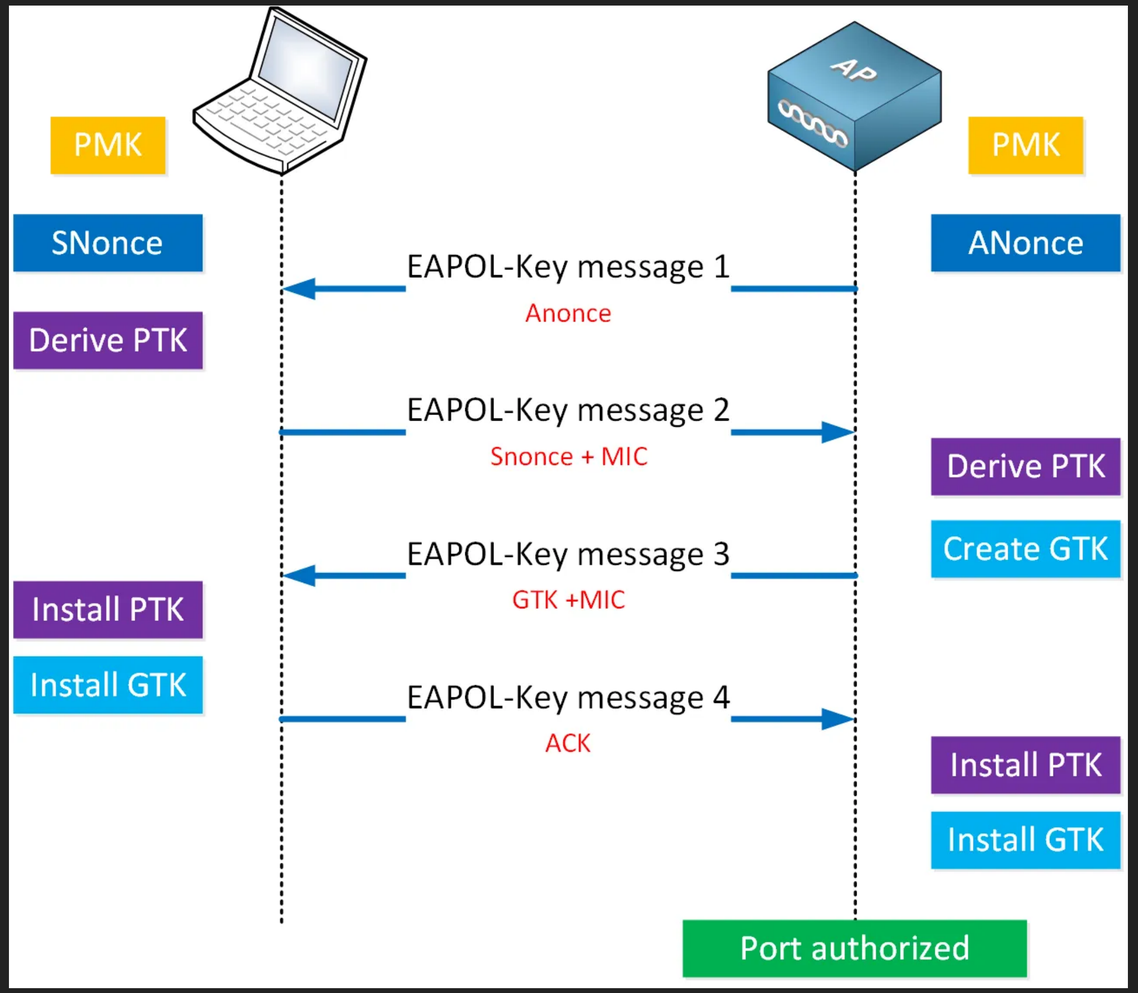
text 收起 換行 複製

```
RadioTap: 00 18 00 00 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Dot11:    80 00 00 00 ff ff ff ff ff ff 12 34 56 78 9a bc 12 34 56 78 9a bc 00 00
Beacon:   00 00 00 00 00 00 00 00 64 00 01 00
SSID:     00 0b 4e 65 76 65 72 20 47 6f 6e 6e 61
```

- **總長度**：約 50-60 位元組（取決於 `RadioTap` 頭部長度）。
- **內容解釋**：
  - `80 00`：信標框架。
  - `ff ff ff ff ff ff`：廣播地址。
  - `12 34 56 78 9a bc`：隨機 MAC（兩次出現，分別為 addr2 和 addr3）。
  - `00 0b`：SSID 長度（11）。
  - `4e 65 ... 61`："Never Gonna" 的 ASCII 編碼。

Wi-Fi Password Cracker

- 名詞解釋
  - PSK（pre-share key）
  - 4-Way Handshake



圖片來源：https://networklessons.com/wp-content/uploads/2023/12/wpa-4-way-handshake-workflow.png

Wi-Fi Password Cracker

- 安全協議
  - WEP：RC4
  - WPA：RC4 + TKIP
  - WPA2：AES（128 bits）
  - WPA3：SAE（256 bits）

Wi-Fi Password Cracker

- 攻擊手法
  - WEP、WPA：爆破 RC4 加密取得 PSK
  - WPA2：使用字典檔或窮舉，離線暴力破解取得 PSK
  - WPA3：降級攻擊、主動式爆破

Wi-Fi Password Cracker

- 防禦方式
  - 高強度密碼
  - 關閉混合模式

https://reurl.cc/LapRe4

Wi-Fi Password Cracker

- // 操作步驟

IR Enumerate

- // 操作步驟

BadUSB

- // 操作步驟

MITM USB

- // 操作步驟

專案資源

https://hackmasterpi.org

https://github.com/1PingSun/HackMaster-Pi

Thank you

Contact

- Email: sunyipingtw@icloud.com
- GitHub: https://github.com/1PingSun
- Blog: https://1ping.org/