CTONE

零成本 pwn 通訊物聯網裝置：入門到放棄

Raagi / 林靜儀

May 16, 2024

$ whoami

- ㄌㄐ / Raagi / Jennifer C Lin / 林靜儀
- 你的水潤餅推廣大使，~~但不是立法委員也不是衛福部次長~~
- Retired CTF player: 10sec, TSJ
- CTOne TR2 team
  - Cybersecurity Researcher
- Research:
  - *I-Soon Internal Documents Leakage Report: Analysis of Wireless Networking Spying Tools and Attacks to Telecommunication Infrastructure*
- This is my first public speech.

CTONE

這場議程的由來是源自於一個我剛入職時的小故事... ...

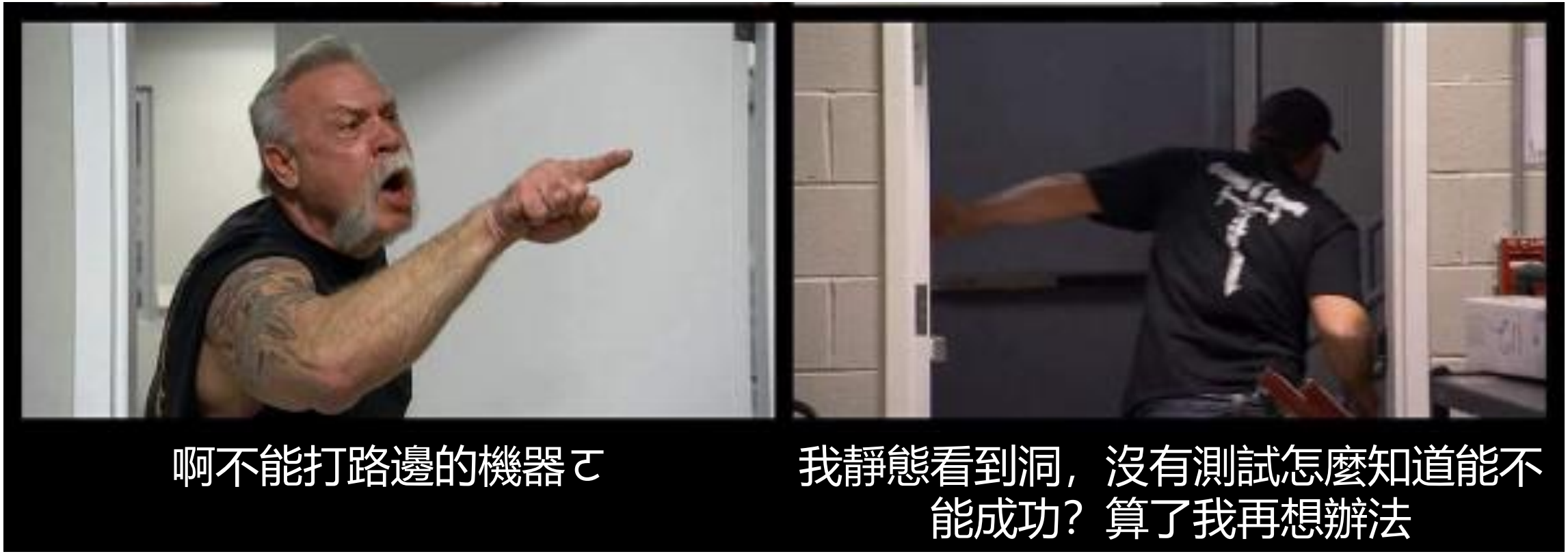
（實際情況沒有迷因那麼火爆。）

CTONE

我們可以買設備，但要買別牌

我可以買這個型號的設備做測試嗎?

4



那沒關係，我自己買一台總行吧

（還有很多較大的廠牌只賣企業訂單）

推廣

Cudy New 5G NR SA NSA AX3000 WiFi 6 CPE 路由器,AX3000 雙卡 5G 行動通訊路由器,Qualcomm IPQ5018,SDX62,4 x 4 MIMO,可拆卸天線,帶鎖,VPN,零層,Cloudflare, P5

★★★★☆ 155

US$499.90

免費送貨5月17日 週五

目的地：台灣

新增至購物車

NETGEAR Nighthawk M6 Pro 行動熱點 5G mmWave,8Gbps,解鎖,AT&T 和 T-Mobile,國際漫遊,便攜式 WiFi 設備,適用於旅行,5G 數據機無線路由器 (MR6500)(翻新)

★★★½☆ 85

過去一個月有500個以上顧客購買

US$174.44 新價格： ~~US$999.99~~

免費送貨5月17日 週五

目的地：台灣

1 個永續屬性

更多購買選擇

US$159.76 (8 項新優惠)

GL.iNet GL-X3000 (Spitz AX) 5G NR AX3000 蜂巢式閘道路由器、Wi-Fi 6 可拆卸式天線、雙 SIM 卡、休旅車、T-Mobile 和 AT&T IoT 裝置認證

★★★★½ 259

過去一個月有200個以上顧客購買

US$489.00 定價: ~~US$519.00~~

省下 US$100.00 使用優惠券

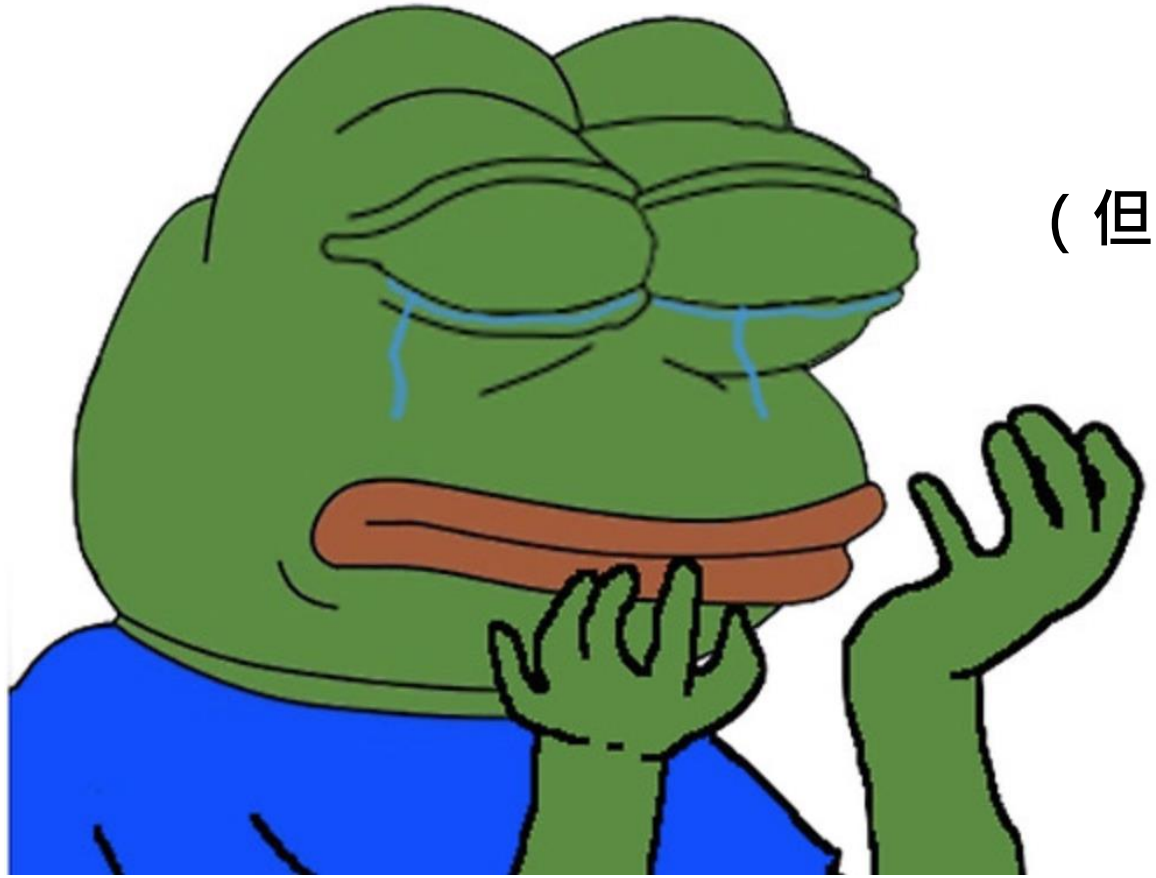
免費送貨5月16日 週四

目的地：台灣

新增至購物車

抱歉，我沒錢

雖然最後研究是有成功進行啦...



（但受限於測試環境只好先找別的目標）

之後在我做其他研究的時候發現了
這個研究...

CTONE

Emulate it until you make it!

Pwning a DrayTek Router before getting it out of the box

Philippe Laulheret (@phLaul)

Senior Security Researcher @ Trellix

12

CTONE

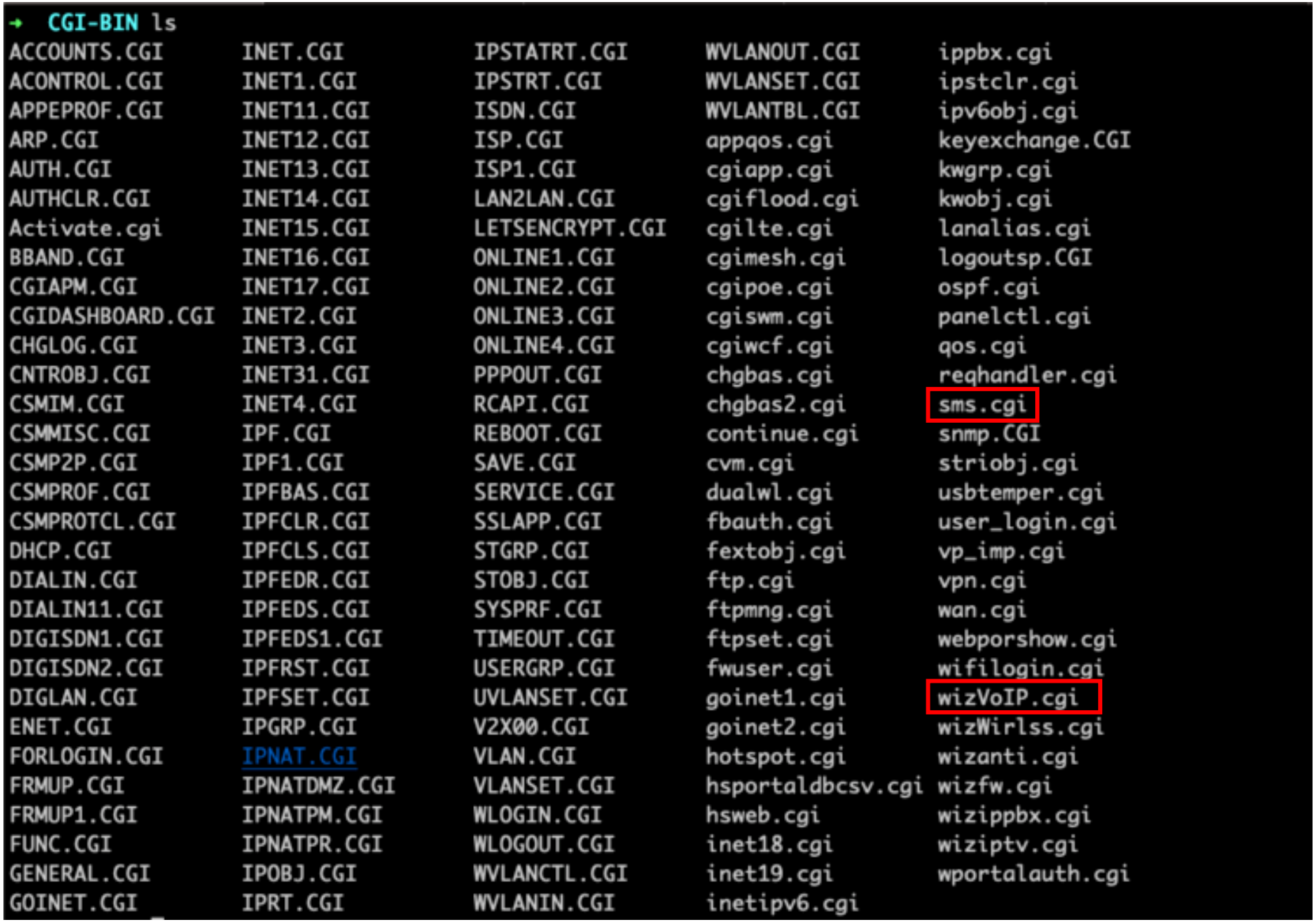
這看起來感覺是我需要的

DrayTek 韌體的特性

- 他分成 MIPS 架構（韌體版本號 2XXX）和 ARM 架構（韌體版本號 3XXX）
- 他有個自己定義的壓縮格式，叫做 PFS file system ，用 binwalk 解不開
  （會被誤認成 Play Station 的韌體）
- **韌體中有提供一個 QEMU script ，作為模擬測試使用，功能也非常齊全**
- 但解開 DrayTek 的韌體有兩個難點
  - MIPS 架構的韌體沒有加密，但是拆開第一層 PFS 後，裡面還有第二層用 customized LZO algorithm 壓縮過的 DrayOS image (sohod64.bin)
  - ARM 架構的韌體，在解開第一層 PFS 後，第二層雖然沒有用 LZO algorithm 壓縮檔案，但有用 ChaCha algorithm 作加密（該篇研究的作者選的是這條路）

我的選擇

- 選擇解開 MIPS 架構的韌體
  - 目前多數支援 4G LTE/5G 網路共享的路由器多數是 MIPS 架構
  - DrayTek Vigor 系列的 4G LTE 路由器也是 MIPS 架構
- 過往我們的研究遇到的難點都是設備環境的 IPC 架構(e.g. ubus)不同導致單純的 user mode emulation 無法運作
  - 之前做法都是把初始化 IPC function call patch 掉，但可能會造成更多不正常的行為
- 在 MIPS 架構上進行 user mode emulation 也會因為不同廠牌的架構略有不同導致無法正常運作
- 我的目標是觀察他們怎麼模擬，如果可以的話我可以 port 到其他設備上，這樣做模擬就能夠測試更多的功能。



```
→  CGI-BIN ls
ACCOUNTS.CGI        INET.CGI          IPSTATRT.CGI      WVLANOUT.CGI      ippbx.cgi
ACONTROL.CGI        INET1.CGI         IPSTRT.CGI        WVLANSET.CGI      ipstclr.cgi
APPEPROF.CGI        INET11.CGI        ISDN.CGI          WVLANTBL.CGI      ipv6obj.cgi
ARP.CGI             INET12.CGI        ISP.CGI           appqos.cgi        keyexchange.CGI
AUTH.CGI            INET13.CGI        ISP1.CGI          cgiapp.cgi        kwgrp.cgi
AUTHCLR.CGI         INET14.CGI        LAN2LAN.CGI       cgiflood.cgi      kwobj.cgi
Activate.cgi        INET15.CGI        LETSENCRYPT.CGI   cgilte.cgi        lanalias.cgi
BBAND.CGI           INET16.CGI        ONLINE1.CGI       cgimesh.cgi       logoutsp.CGI
CGIAPM.CGI          INET17.CGI        ONLINE2.CGI       cgipoe.cgi        ospf.cgi
CGIDASHBOARD.CGI    INET2.CGI         ONLINE3.CGI       cgiswm.cgi        panelctl.cgi
CHGLOG.CGI          INET3.CGI         ONLINE4.CGI       cgiwcf.cgi        qos.cgi
CNTROBJ.CGI         INET31.CGI        PPPOUT.CGI        chgbas.cgi        reqhandler.cgi
CSMIM.CGI           INET4.CGI         RCAPI.CGI         chgbas2.cgi       sms.cgi
CSMMISC.CGI         IPF.CGI           REBOOT.CGI        continue.cgi      snmp.CGI
CSMP2P.CGI          IPF1.CGI          SAVE.CGI          cvm.cgi           striobj.cgi
CSMPROF.CGI         IPFBAS.CGI        SERVICE.CGI       dualwl.cgi        usbtemper.cgi
CSMPROTCL.CGI       IPFCLR.CGI        SSLAPP.CGI        fbauth.cgi        user_login.cgi
DHCP.CGI            IPFCLS.CGI        STGRP.CGI         fextobj.cgi       vp_imp.cgi
DIALIN.CGI          IPFEDR.CGI        STOBJ.CGI         ftp.cgi           vpn.cgi
DIALIN11.CGI        IPFEDS.CGI        SYSPRF.CGI        ftpmng.cgi        wan.cgi
DIGISDN1.CGI        IPFEDS1.CGI       TIMEOUT.CGI       ftpset.cgi        webporshow.cgi
DIGISDN2.CGI        IPFRST.CGI        USERGRP.CGI       fwuser.cgi        wifilogin.cgi
DIGLAN.CGI          IPFSET.CGI        UVLANSET.CGI      goinet1.cgi       wizVoIP.cgi
ENET.CGI            IPGRP.CGI         V2X00.CGI         goinet2.cgi       wizWirlss.cgi
FORLOGIN.CGI        IPNAT.CGI         VLAN.CGI          hotspot.cgi       wizanti.cgi
FRMUP.CGI           IPNATDMZ.CGI      VLANSET.CGI       hsportaldbcsv.cgi wizfw.cgi
FRMUP1.CGI          IPNATPM.CGI       WLOGIN.CGI        hsweb.cgi         wizippbx.cgi
FUNC.CGI            IPNATPR.CGI       WLOGOUT.CGI       inet18.cgi        wiziptv.cgi
GENERAL.CGI         IPOBJ.CGI         WVLANCTL.CGI      inet19.cgi        wportalauth.cgi
GOINET.CGI          IPRT.CGI          WVLANIN.CGI       inetipv6.cgi
```


CTONE

而解開之後的 /vqemu/runlinux.sh

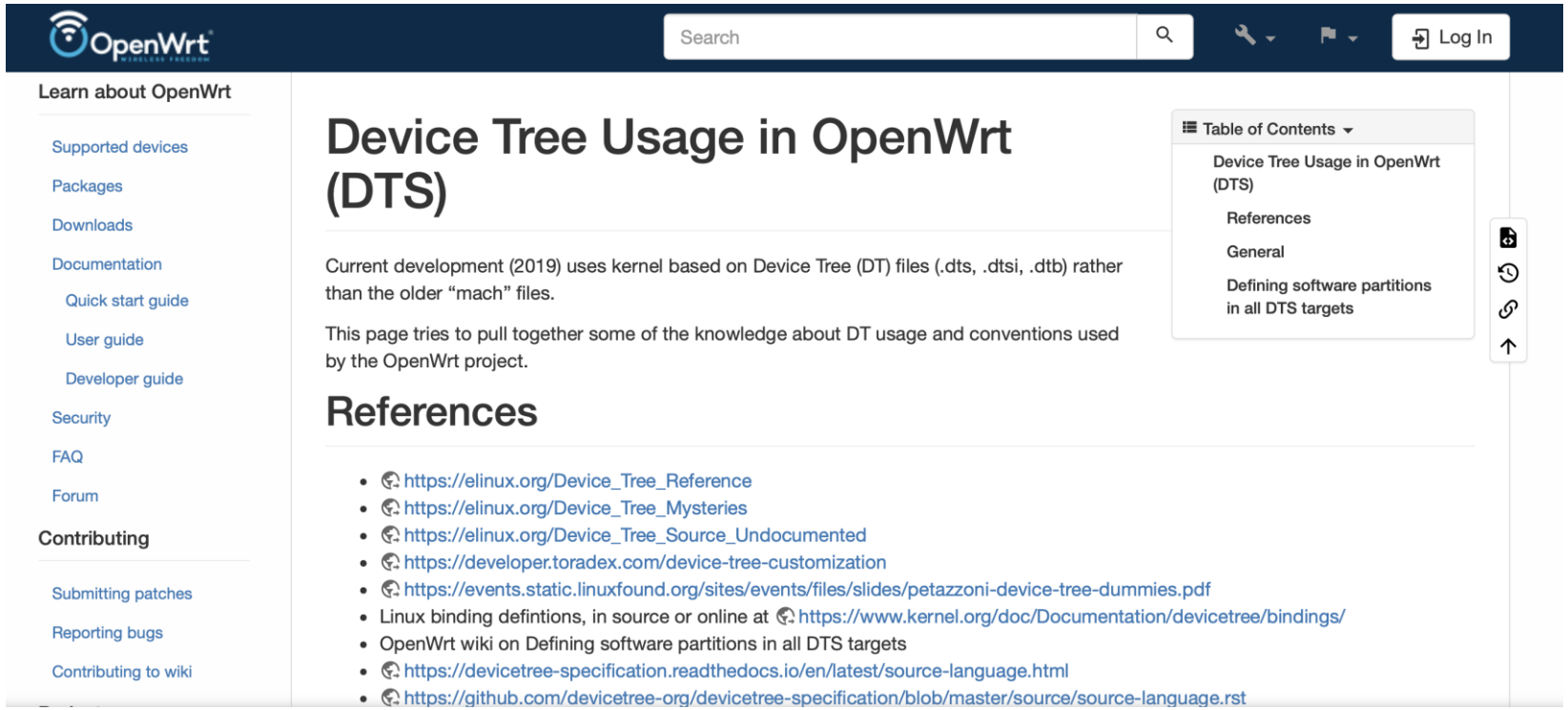
```
1 qemu.sh                                                    Buffers
24 GCI_PATH="./app/gci"
23 GCI_FAIL="./app/gct_exp_fatl"
22 GDEF_FILE="$GCI_PATH/draycfg.def"
21 GEXP_FLAG="$GCI_PATH/EXP_FLAG"
20 GEXP_FILE="$GCI_PATH/draycfg. exp"
19 GDEF_FILE_ADDR="0x4de0000"
18 GEXP_FLAG_ADDR="0x55€0000"
17 GEXP_FILE_ADDR="0x550010"
16 echo "kyrofang" > $GDEF_FILE
15 echo "0#" > $GEXP_FLAG
14 #echo "19831026" > $GEXP_FILE
13 # Make sure the lan works... shrug lol
12 (sleep 20 && ethtool -K qemu-lan tx off)&
11 #-netdev tap, id=network-lan, ifname=qemu-lan, script=no,downscript=no \
10 # -cpu host \
 9 # - -enable-kvm \
 8 #
 7 -dtb DrayTek
 6 /qemu-system-aarch64 daytek -M virt, gic_version=3
 5 - cpu 24KEc \
 4 -m 1024
 3 -dtb DrayTek
 2 - kernel ./vqemu/sohod64.bin $serial_option \
 1 - nographic $gdb_serial_option $gdb_remote_option \
25  -device virtio-net-pci,netdev=network-lan,mac=${LAN_MAC} \
 1 -netdev tap, id=network-lan, ifname=qemu-lan, script=no, downscript=no \
1 * qemu.sh  sh  ❖ ⓢ                                  utf-8  25: 48  Top
```

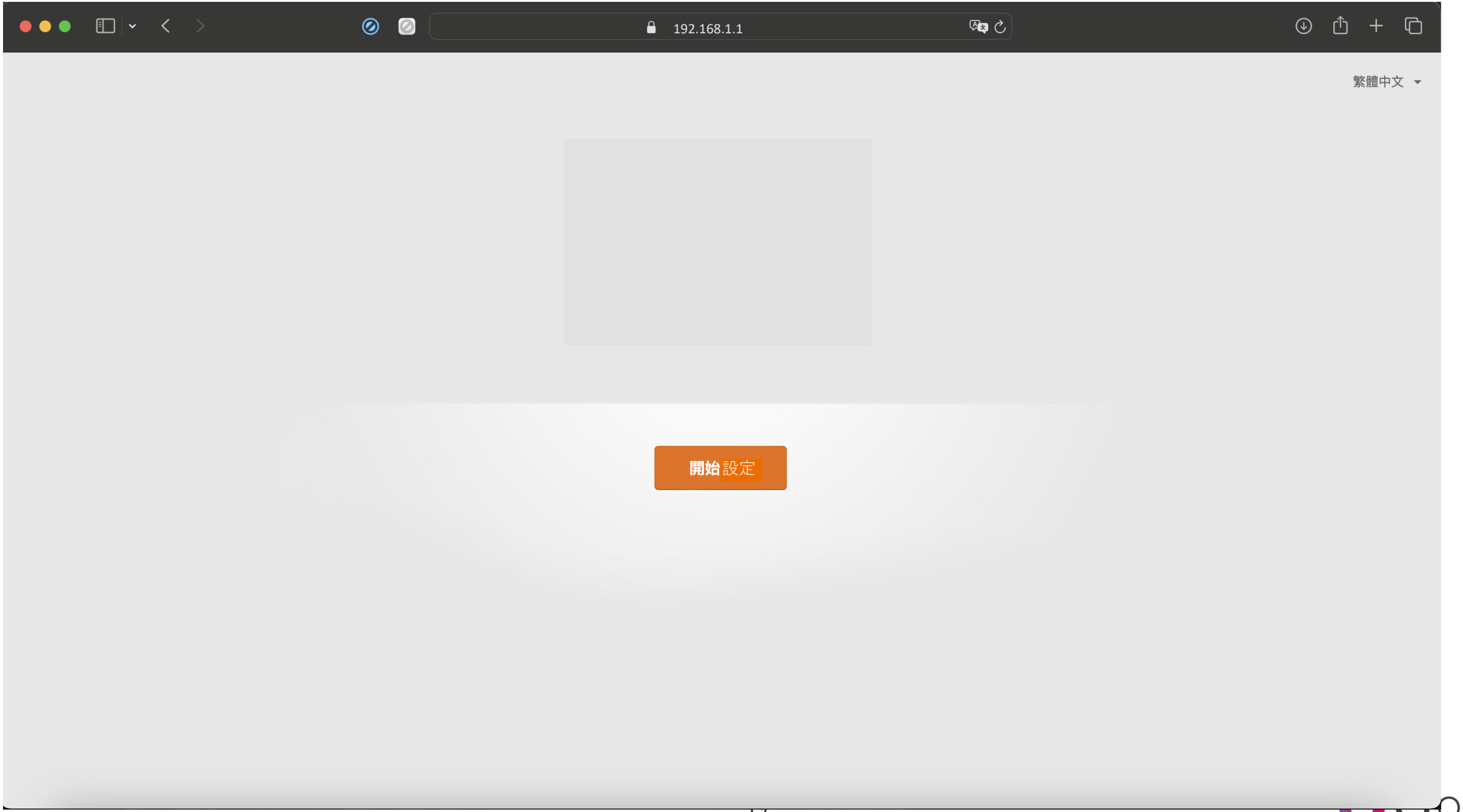
hardware offloading

CTONE

如法炮製一樣的 qemu script

- 觀察是否存在 libubus, ubusd, libdbus, dbusd 等可以分辨其 IPC interface
  - e.g. 若有 libubus 就可以分辨出他是一個 openwrt-based 的韌體，模擬時需要 dtb file 可以在 openwrt forum 找到





我們發現到的問題

CTONE

SMS server, sendSMS.js

- 使用 4G LTE 或 5G SIM 卡作為網路介面的路由器，通常會有 SMS server，原因是為了支援使用 SMSoIP 收發訊息的使用者們的 SMS gateway 。
- SMS server 常見的實作方式是使用一個叫做 smstools 的開源專案（smstools2 在 2003 年專案被棄置，之後接手的專案是 smstools3，但最近一次的 commit 也在 2007 年），當中使用比較舊版本實作的案例中，SMS header parser 在處理字串時也有不嚴謹的地方。
- 另外為了能夠從 web GUI 設定和檢視 SMS server 的狀態，通常會有一個 interface 叫作 sendsms.js ，也會 parse SMS 的 header 和 body ，並印在 web GUI 的畫面上，可以看到從哪裡收到了什麼內容的 SMS 訊息
- 而一部分案例中，若在 SMS 內文中寫入 XSS payload ，就會在 web GUI 上觸發

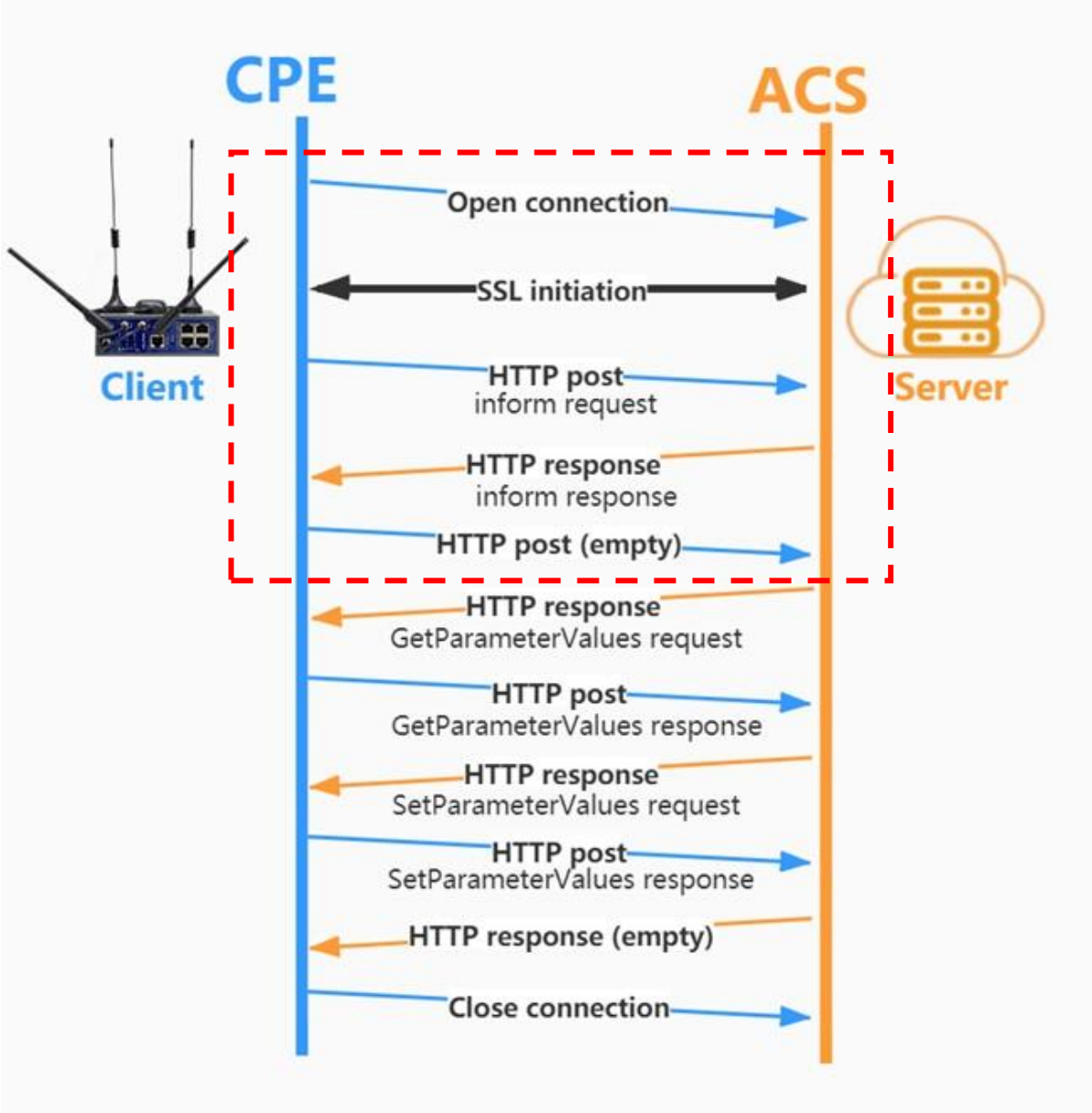
21

CWMP configuration, customized CWMPd

- iptables 的設定不夠嚴謹，允許外部對 port 7574 連線
- CWMP protocol 傳遞的格式是 XML ，而許多的設備中的 CWMPd 的 XML parser 對於字串處理不夠嚴謹

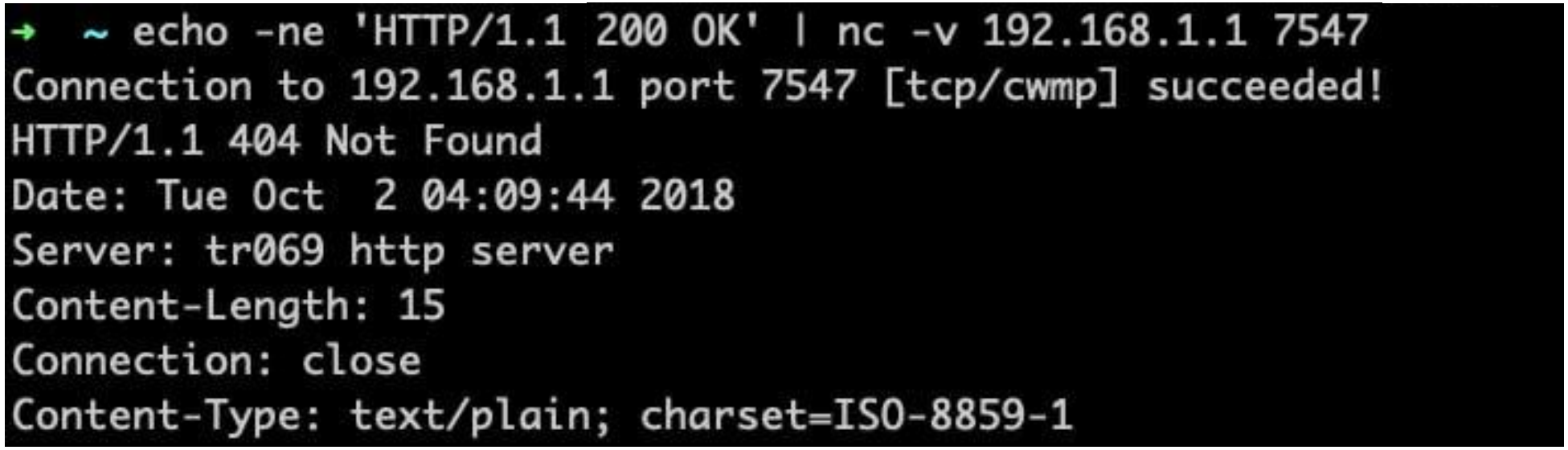
CTONE

CWMP protocol



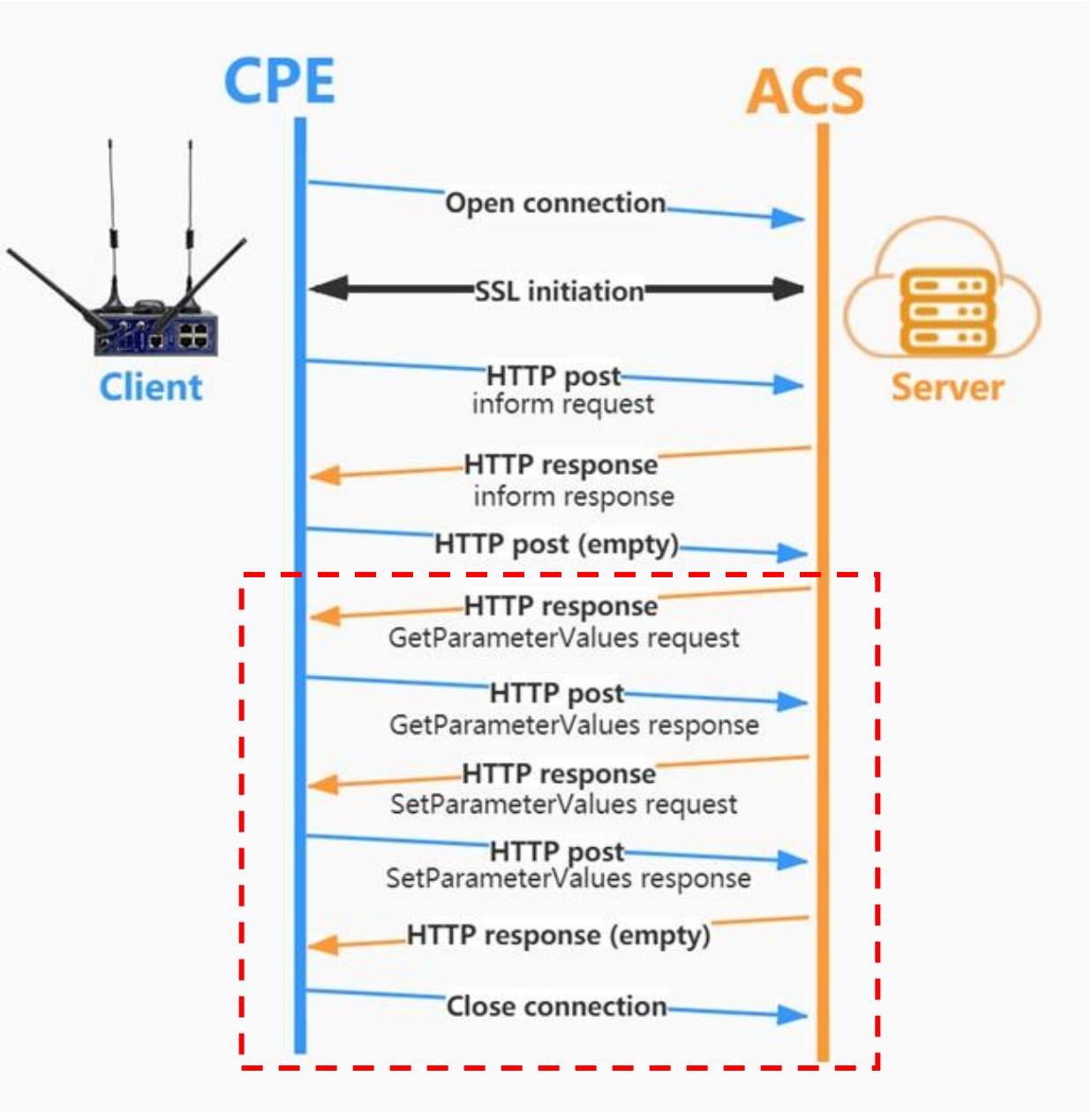
Example

- 當下的思路：因為 iptables 的設定對於從外部進來的流量全部 ACCEPT，那麼就試試看傳送一個 INFORM REPLY(只有 ACS 才能發送 INFORM Reply，body 會有一段 XML payload) 看會有什麼樣的結果，以確定他有沒有做驗證。
- 我先送一個沒有包 XML 的 200 OK ，沒想到他也回我一個 HTTP Reply？



Example

- 後來再仔細測試了幾個常見的 command，發現可以繞過上面驗證發送 request 的是否為被授權的 ACS ，並直接對設備的設定進行更改、或取得一些機密資訊 (e.g. GetParameterValues)



結論

- 使用模擬的方式做研究其實是萬不得已的下下策
  - 前面提到關於不同廠牌的晶片架構的指令集實作不同的問題在 system mode emulation 依然有機率會遇到問題（尤其 mipsel 架構的設備）
  - 因為有部分硬體缺失，必須做 hardware offloading ，但無法確保是否與真實的環境的測試結果相符
- 但模擬的好處：
  - 可以更廣泛的調查特定類別的設備可能有什麼樣的功能值得作為研究的目標
  - 成本低廉
  - 測試容錯的機會更多
- 可以做為之後要實體測試前一個測水溫的步驟

其他可以協助模擬的工具

- FAT.py
- Firmadyne
- Firmadyne/libnvram.so（尤其在測試 ASUS 的設備時特別有用）

CTONE

Reference

[1] Emulate it until you make it! Pwning a DrayTek Router before getting it out of the box

[2] Device Tree Usage in OpenWrt (DTS) – OpenWRT Forum

[3] TR-069 Amendment 6: CPE WAN Management Protocol – BBF

[4] IoT Exploitation - Red Teaming and Malware Analysis(GitBook)

CTONE

CTONE

Thank You!