COSCOP 2007

Router Hacking 101

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

此簡報不公開下載，請來信索取

Overview

- Possibilities to hacking the routers with open source software.
- OpenWRT 101
  - Overall Introduction
  - Supported Hardware
  - Howto Shell Access / Reflash the images
- Projects and hacking in the communities

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

Open source Communities for WiFi routers

- OpenWRT http://www.openwrt.org
- DD-WRT (not that opensource but a lot of features) http://www.dd-wrt.org/
- X-WRT (enhanced webif based on opnewrt) http://x-wrt.org/
- Tomato (HyperWRT-based firmware aimed to be easy, stable and fast) http://www.polarcloud.com/tomato
- Communities for ASUS routers http://wl500g.info/

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

OpenWRT 101

- A linux distribution for embedded system, provide a well designed building system.
- It's now supporting more then 10 different hardware platforms.
- It's commercialized in the mass market.
- Two major version - White Russian and Kamikaze

白色俄羅斯, White Russian

- 5.0 cl (5 parts) Vodka
- 2.0 cl (2 parts) Coffee liqueur
- 3.0 cl (3 parts) Fresh cream

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

白色俄羅斯, White Russian

- 支援數種平台
  - Broadcom 47xx,57xx,63xx 為主支持平台, x86, Mikrotik RB532, TI AR7, Aruba, Atheros AR531x
- 較為完整的 event handing 機制
- Web Interface

神風特攻隊，Kamikaze

- 3cl (1 part) Vodka 伏特加
- 3cl (1 part) triple sec 橙味利口酒 (或叫白橙皮)
- 3cl (1 part) lemon juice 檸檬汁

http://en.wikipedia.org/wiki/Kamikaze_(cocktail)

神風特攻隊，Kamikaze

- 支援更多平台
  - 避免 Broadcom 平台專屬工具
- 更强大的網路設定檔 (/etc/config/network)
  - 支援 VLANs, Bridging, 完整的 WLAN 設定如 802.11x 等
- 新的編譯系統 (multiple profiles for same platform)

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

http://en.wikipedia.org/wiki/Kamikaze_(cocktail)

Structure of the Buildroot

- Source directories
  - toolchain/ (kernels, binutils, gcc, uClibc)
  - package/
  - target/
  - scripts/
- Build directories
  - toolchain_build_<arch> /
  - staging_dir_<arch> /
  - build_<arch> /

Build packages and images

- Suggested platform: Debian Etch. (IMHO)
- make menuconifg && make
    - unpacks kernel headers
    - builds binutils
    - builds initial gcc
    - uses initial gcc to build uClibc
    - builds nal gcc
    - (optional) builds binutils
    - builds packages
    - builds kernel
    - builds firmware image.

Package systems

- Based on ipkg
  - A very lightweight package management system
  - http://handhelds.org/moin/moin.cgi/Ipkg
- FreeBSD ports/Gentoo packages style building system
  - GNU Makefile rules!
  - automaticly download the source tarball, untar, compile and pack it!
  - handles package dependencies!

New platform support and profiles mechanism

- target/linux/*/
  - target/linux/*/config/
  - target/linux/*/profiles
- One hardware platform but support many different products or applications.

Supported platforms aka 台灣入手容易度

- Linksys WRT54G series
  - Warning: a lot of fake products from china

- ASUS WL-700gE
- Atheros-based hardware
  - Meraki
  - FON

- Check http://wiki.openwrt.org/TableOfHardware for more details

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

Meraki Mini

Bootloader: RedBoot

CPU: Atheros AR2315

CPU Speed: 180 Mhz

Flash size: 8 MB

RAM: 32 MB

Wireless: integrated Atheros 802.11b/g

Ethernet: 1xLAN

Serial: yes

JTAG: yes

LaFonera

Architecture MIPS 4KEc

Bootloader RedBoot

System-On-Chip Atheros AR2315

CPU Speed 183 MHz

Flash size 8 MiB

RAM 16 MiB

Wireless Integrated Atheros 802.11b/g

Ethernet 1x RJ45

Serial Yes

JTAG No

LaFonera+

Architecture MIPS 4KEc

Bootloader RedBoot

System-On-Chip Atheros AR2315

CPU Speed 183 MHz

Flash size 8 MiB

RAM 16 MiB

Wireless Integrated Atheros 802.11b/g

Ethernet 2x RJ45

Serial Yes

JTAG No

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

Big Fat Disclaimer

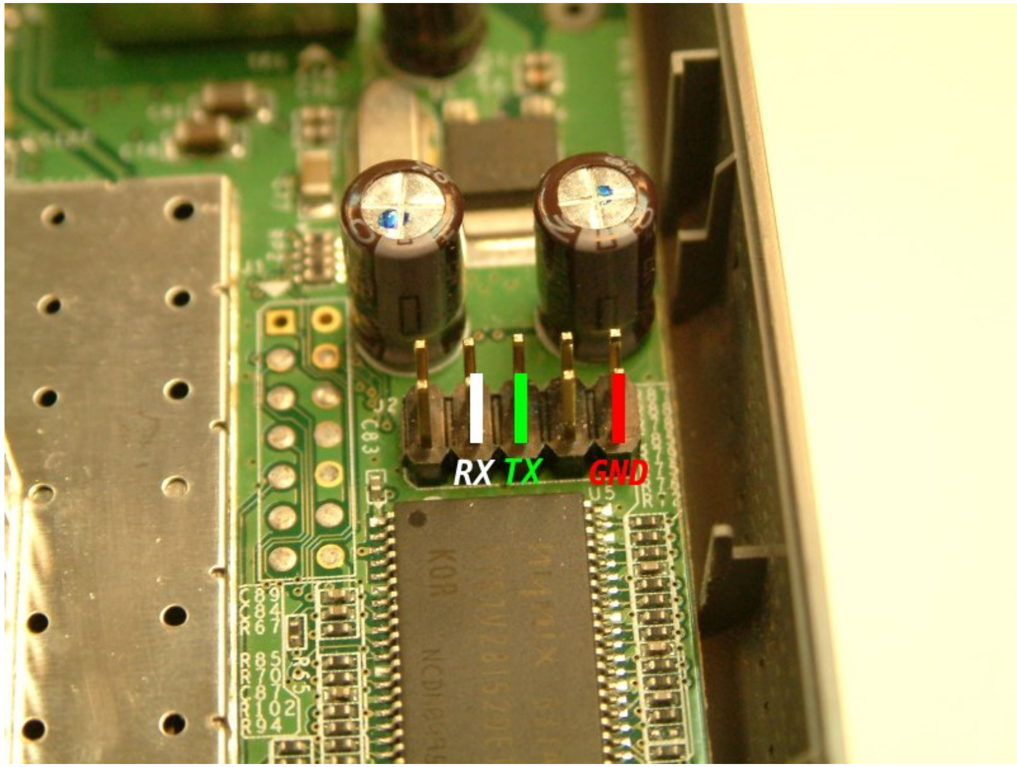
- 磚化危險，保固自理

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

Routers with openwrt for Mass market

- Meraki mini
  - http://dl.meraki.net/linux/openwrt-meraki.tar.gz
  - http://dl.meraki.net/linux/meraki-linux-2.6.16.16-beta-1.0.tar.gz
  - http://dl.meraki.net/linux/redboot_mini.tar.gz
- FON
  - LaFonera
    - http://download.fon.com/firmware/fonera/latest/fonera.tar.bz2
  - LaFonera+
    - http://download.fon.com/firmware/foneraplus/latest/foneraplu

Access to redboot by serial console.



- Nokia 手機傳輸線 CA-42
- 市價約 150-300
- 可用於 LaFonera 與 LaFonera+
- 細節請參看 http://0rz.tw/be3fM

Unlocking LaFonera Plus

- redboot and telnet function
- Requirements
  - telnet and tftp server on your workstation.
  - A script to connect to 192.168.1.1 port 9000 at the first 3 seconds after the router boots up.

細節請參考
http://www.fonboard.nl/wiki/HowTo_Foneraplus_unlocking/en
關於 redboot 指令請參考
http://sourceware.org/redboot/

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

Screenshot of telnet into redboot

```
ARPING 192.168.1.1 from 192.168.1.254 eth0
Unicast reply from 192.168.1.1 [XX:XX:XX:XX:XX:XX]  0.992ms
Sent 9 probes (9 broadcast(s))
Received 1 response(s)
fonera [192.168.1.1] 9000 (?) open
== Executing boot script in 0.890 seconds - enter ^C to abort
^C
RedBoot>
sent 6, rcvd 82
Trying 192.168.1.1...
Connected to 192.168.1.1.
Escape character is '^]'.
RedBoot>
```

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

Reflash 101

```
RedBoot> fis list
Name              FLASH addr  Mem addr    Length      Entry point
RedBoot           0xA8000000  0x80040400  0x00030000  0xA8000000
loader            0xA8030000  0x80100000  0x00010000  0x80100000
image             0xA8040000  0x80040400  0x00230004  0x80040400
image2            0xA8660000  0xA8660000  0x00140000  0x80040400
FIS directory     0xA87E0000  0xA87E0000  0x0000F000  0x00000000
RedBoot config    0xA87EF000  0xA87EF000  0x00001000  0x00000000
RedBoot> load -r -b 0x80100000 image.bin
Using default protocol (TFTP)
Raw file loaded 0x80100000-0x8070ffff, assumed entry at 0x80100000
RedBoot>  fis write -b 0x80320000 -f 0xa8260000 -l 0x003f0000
* CAUTION * about to program FLASH
        at 0xa8260000..0xa864ffff from 0x80320000 - continue (y/n)? y
... Erase from 0xa8260000-0xa8650000: ..........................................................
... Program from 0x80320000-0x80710000 at 0xa8260000: ..............................................
.............
RedBoot> reset
```

http://www.fonboard.nl/wiki/HowTo_Foneraplus_unlocking/en
http://wiki.openwrt.org/OpenWrtDocs/Hardware/Fon/Fonera

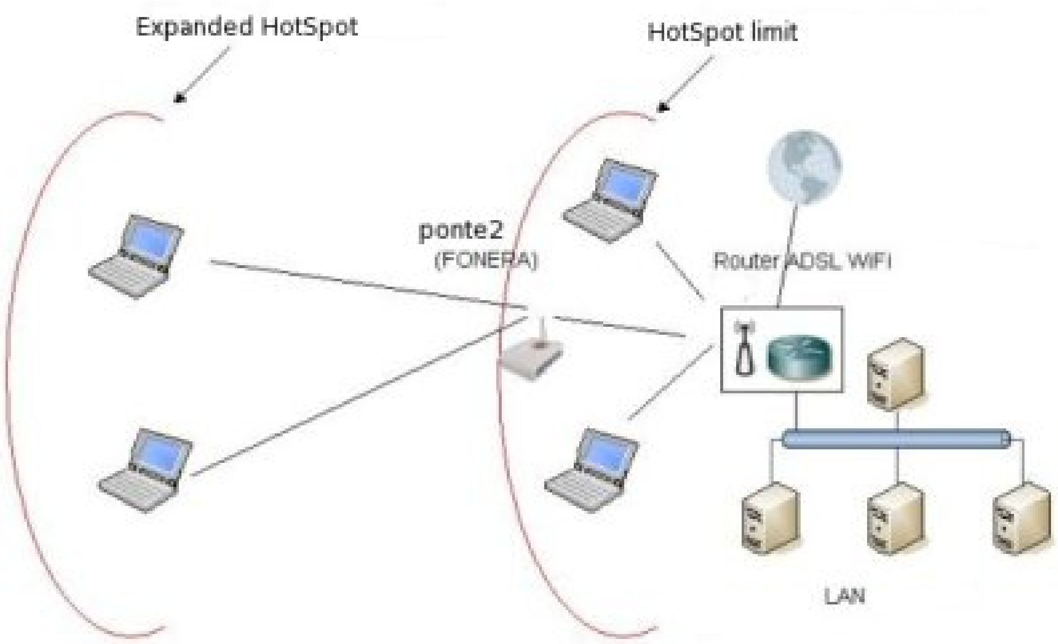
FON hacking communities

- DD-WRT
  - a lot of strange ideas on the forum.
  - the information are collected on the wiki
  - http://www.dd-wrt.com/wiki/index.php/Fonera

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

FON hacking communities

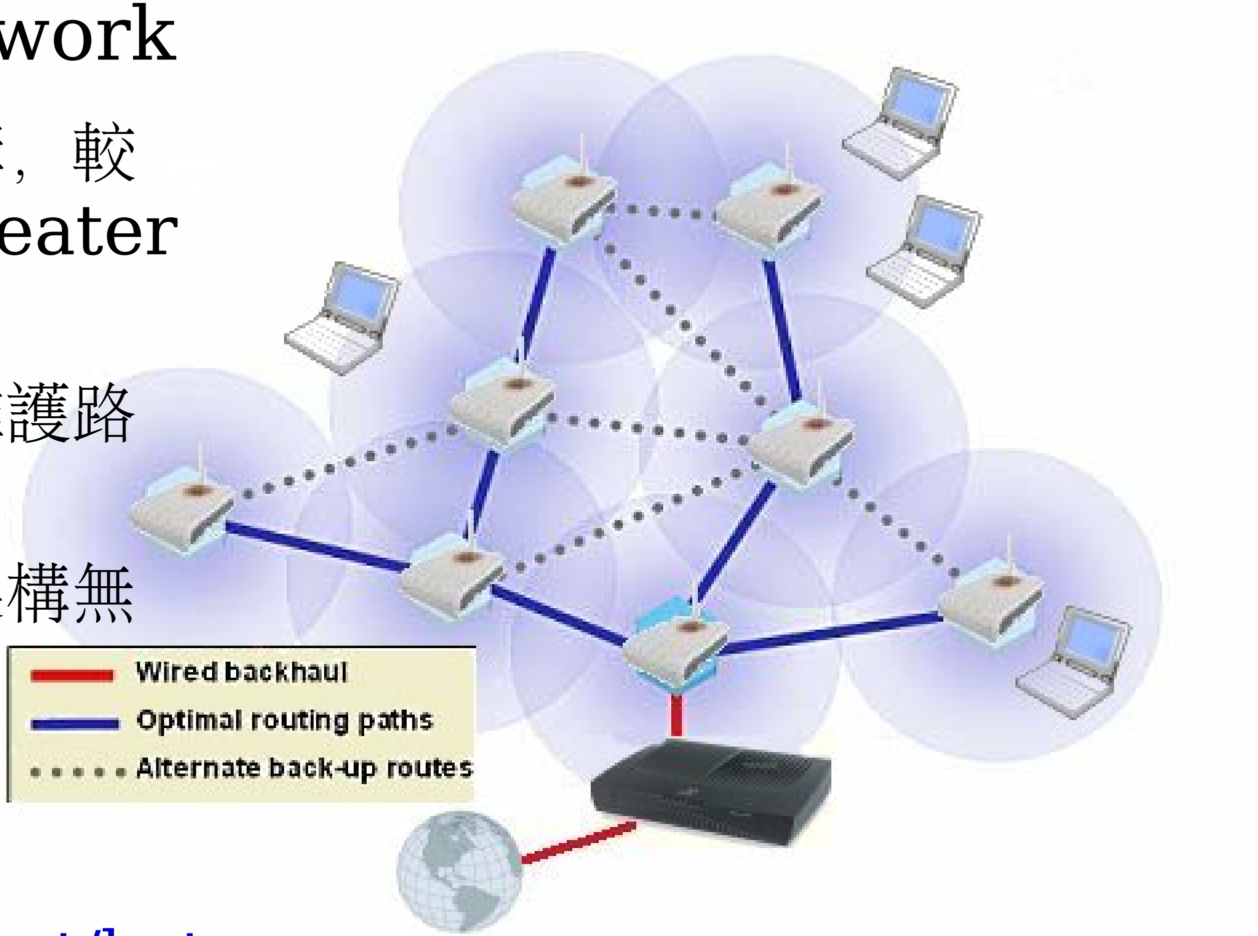
- RO.B.IN / Ponte by Antonio Anselmi
  - Repeater, FON expander, mesh network
  - Integrated with ROBIN (ROuting Batman Inside)
  - http://www.blogin.it/



Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

ponte2 mesh

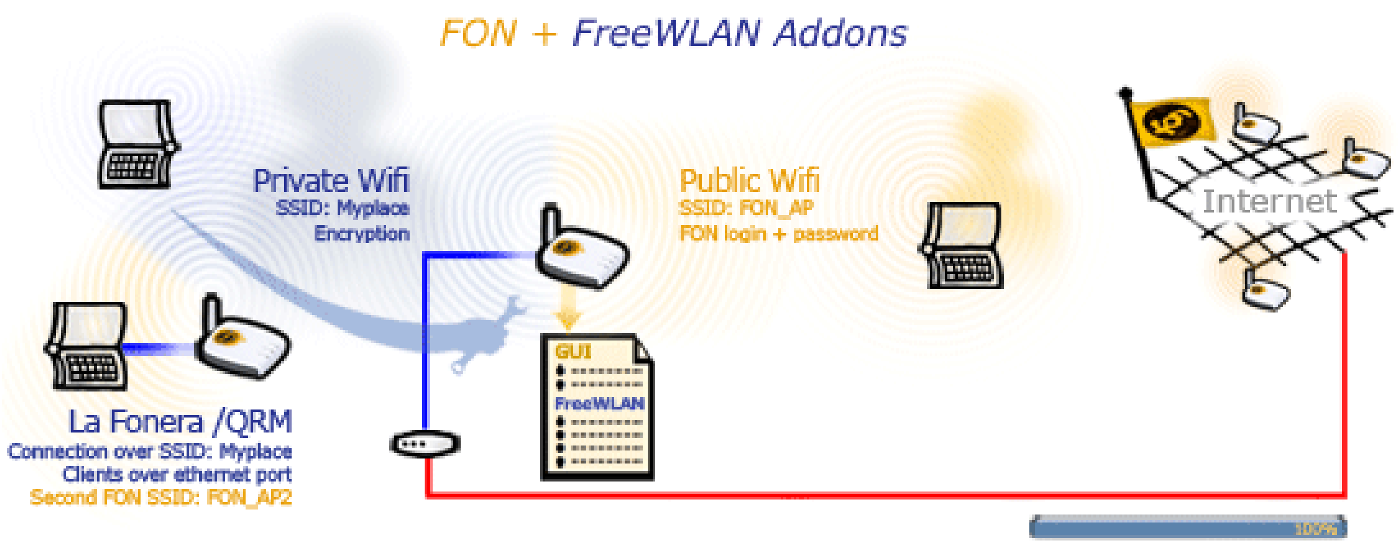
- Wireless mesh network
  - 點對點的無線網路架構，較傳統的 wireless repeater 容易佈建與維護
  - 因為點與點間會自行維護路由、資料傳輸方式等
  - 可以較為節省的方式架構無線網路



http://www.open-mesh.net/batman

The other communies

- FrancoFON (In franch) http://www.francofon.fr/
  - Enhanded WebIF and features on LaFonera
  - Integrated with RO.B.IN / Ponte2
- FreeWLAN Addons (German Developer but English documents!) http://trac.freewlan.info/



Applications with OpenWRT

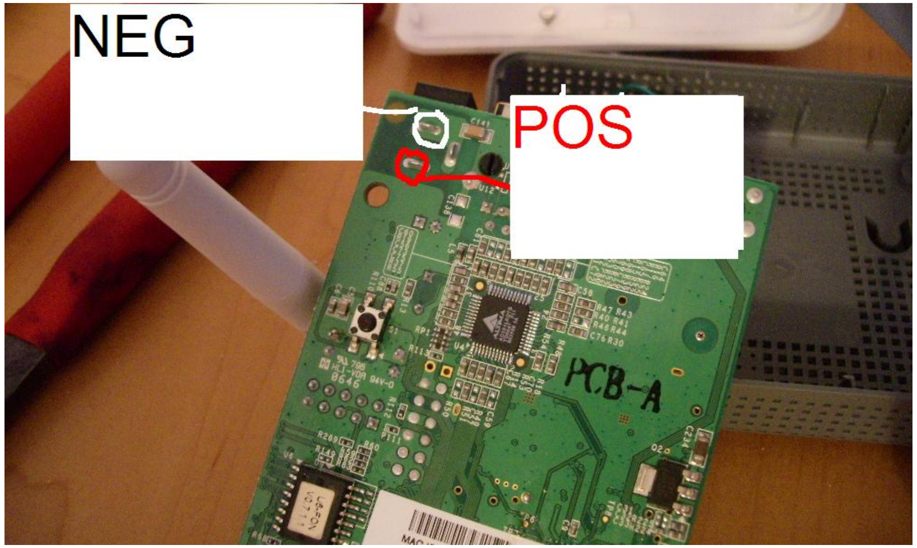
- Virtual Private Network system
- Network File Server (ftp, samba)
- Mobile AP
- Multimedia system/Streaming Server/Music Player
- Printer sharing
- Leecher/File downloader/BT on routers.

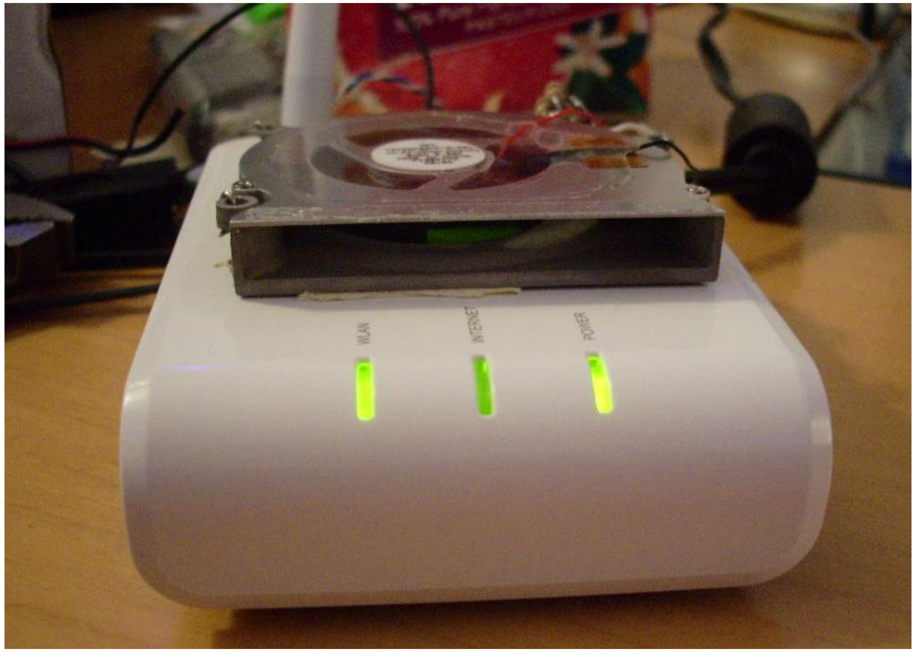
Porta2030

http://porta2030.tossug.org

Introducted by Macpaul in the OSDC this year.

LaFonera cooling system





http://www.dd-wrt.com/wiki/index.php/LaFonera_Hardware_Cooling-System

Hardware hacking- more storage

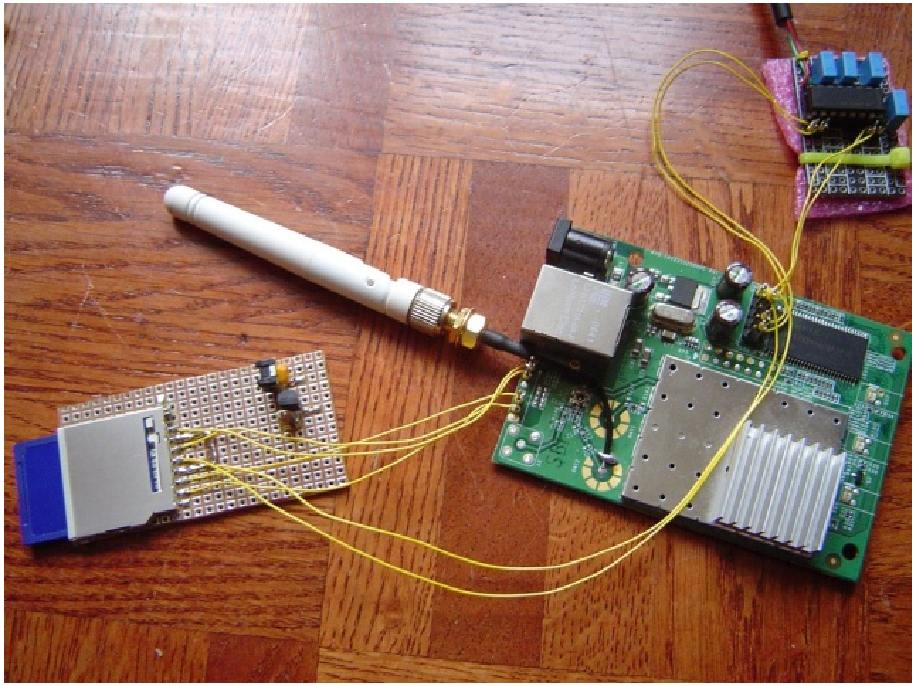
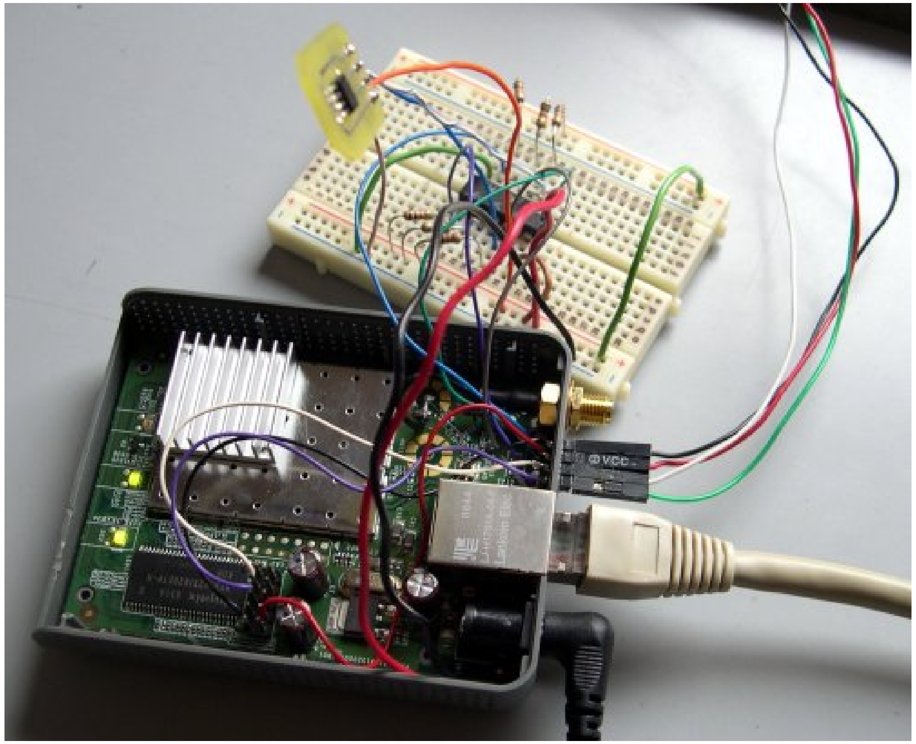
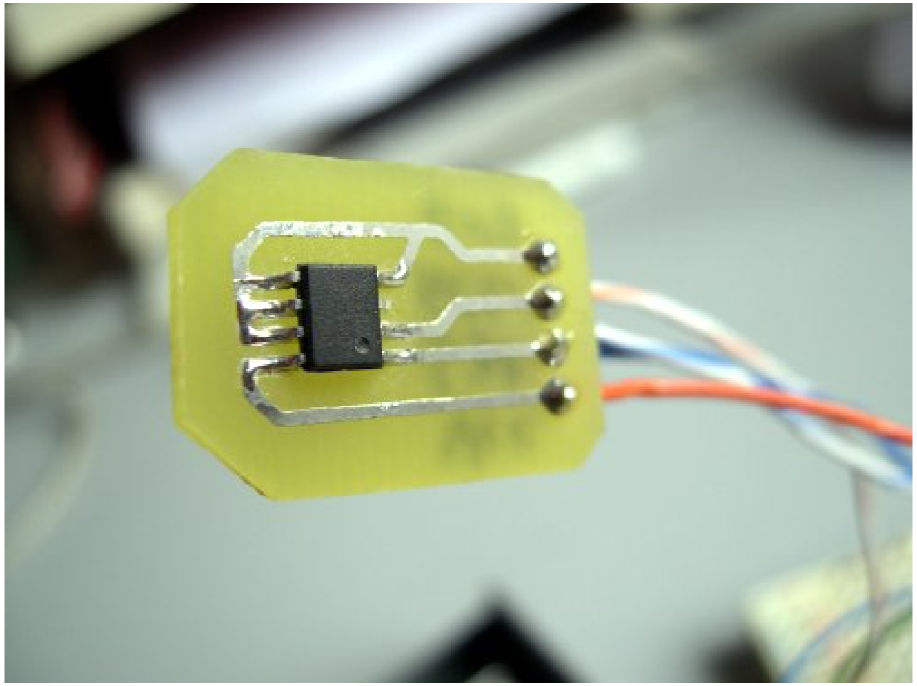


Image Source: Fonera SD Card Hack
by Jkxhttp://www.larsen-b.com/

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

Hardware hacking- thermograph via i2c





http://www.lefinnois.net/wp/index.php/2007/05/05/un-bus-i2c-pour-la-fonera/

Second Antennas

http://www.dd-wrt.com/wiki/index.php/LaFonera_Hardware_Second-Antenna

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

ASUS WL-500gP

- OpenWrt Kamikaze
- X-Wrt Extensions 7.07
- Features
  - Bittorrent – mldonkey
  - Hotspot management – chillispot
  - FON friendly

by 鄉民 DearKurt
my.ipod.shuffle@gmail.com

http://www.foniao.net/phpbb/viewtopic.php?p=5118#5118

Questions ?

Thank you!

Rex Tsai
chihchun@kalug.linux.org.tw
http://people.debian.org.tw/~chihchun/

Web 2.0 and WiFi Networks

- OpenID WiFi
- Social WiFi Network - CoovaAAA with Facebook

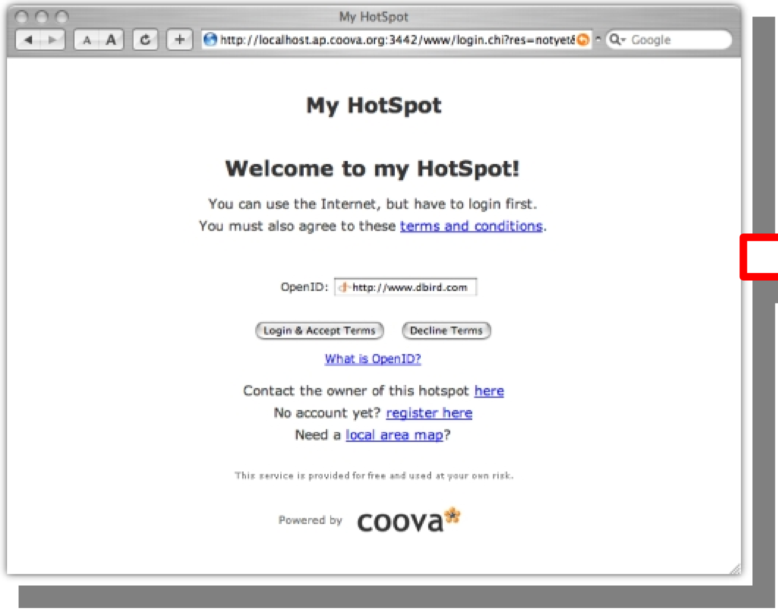
These ideas are created and implemented by
David Bird <david@coova.com> of
Coova Project. http://www.coova.org/

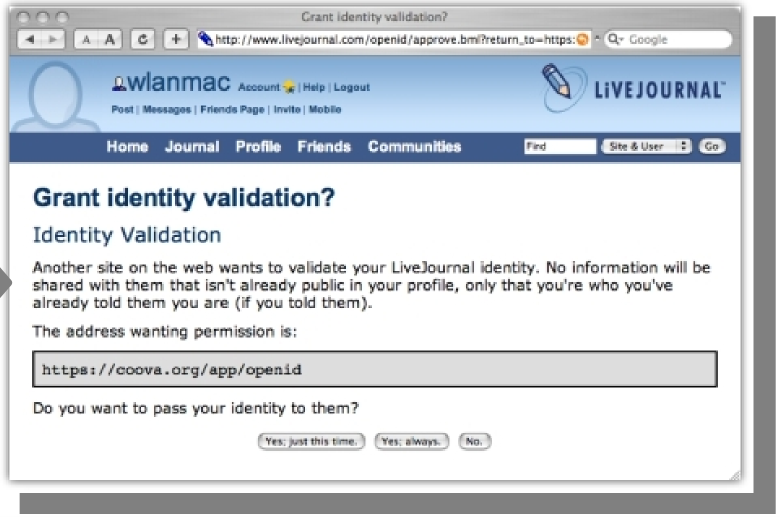
OpenID

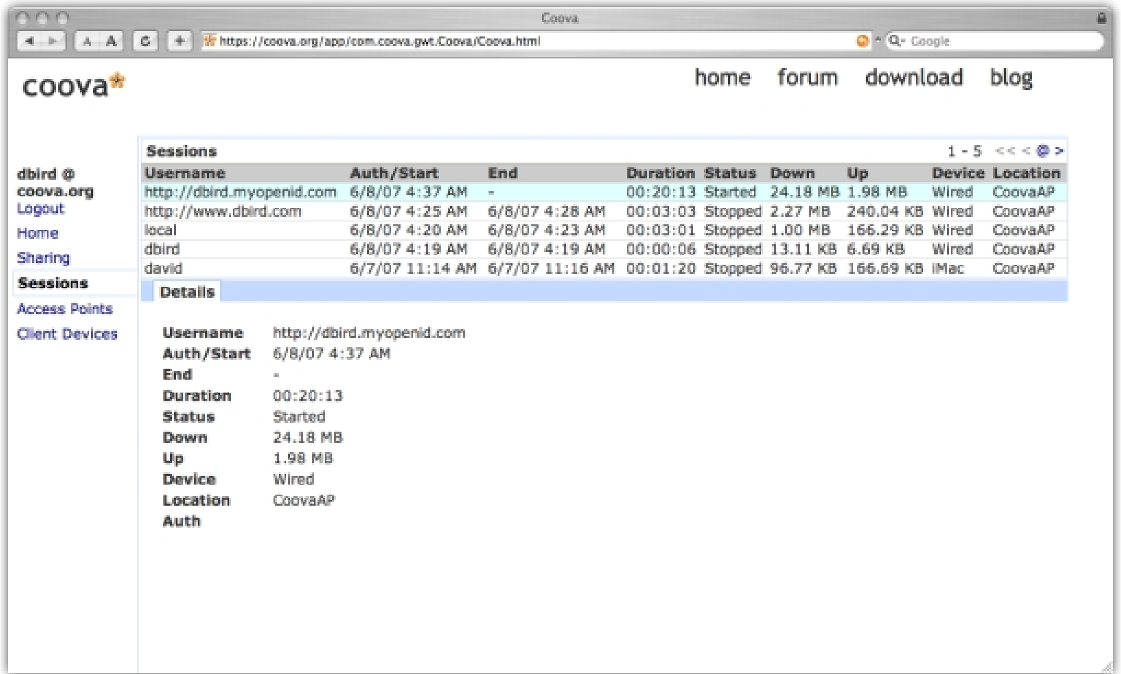
- OpenID 是分散式身份認證協定，透過網址作為你的身份確認 (identity) 機制。你可用同一個身份登入數種不同網站，而不需老是重新註冊新帳號。

  http://zh.wikipedia.org/w/index.php?title=OpenID&variant=zh-tw

Screenshot of Coova's OpenID implementation







Facebook

- 目前其中一個最大的 Social networking website
- 眾多網友在上面無聊的戳戳與玩小程式
- 提供開發者平台，可撰寫小程式或整合第三方網站系統 http://developers.facebook.com

http://www.facebook.com/

Screenshot of Facebook enanbled hotspot