

**Open Razzmatazz Laboratory (OrzLab)**

<http://orzlab.blogspot.com/>  **orzLab**

# 電信通訊的自由與 安全議題

July 22, 2007

Jim Huang( 黃敬群 /jserv)

Email: <[jserv.tw@gmail.com](mailto:jserv.tw@gmail.com)>

<[jserv@openmoko.org](mailto:jserv@openmoko.org)>

Blog: <http://blog.linux.org.tw/jserv/>

# 自我介紹

- OpenMoko 開發者
- 手機 /PDA、 Mobile TV/ 數位電視代工設計
- 參與自由軟體開發
  - 新酷音輸入法
  - Kaffe.org / GNU Classpath
  - ... (<http://jserv.sayya.org/> for details) ...
- 專業熱血工讀生

# 提綱

- 通訊裝置背後的議題
- 電信通訊的自由開放
- 安全性挑戰



# • 複雜性、多樣性

- 高度整合
- 五花八門

# 行動電話的時代

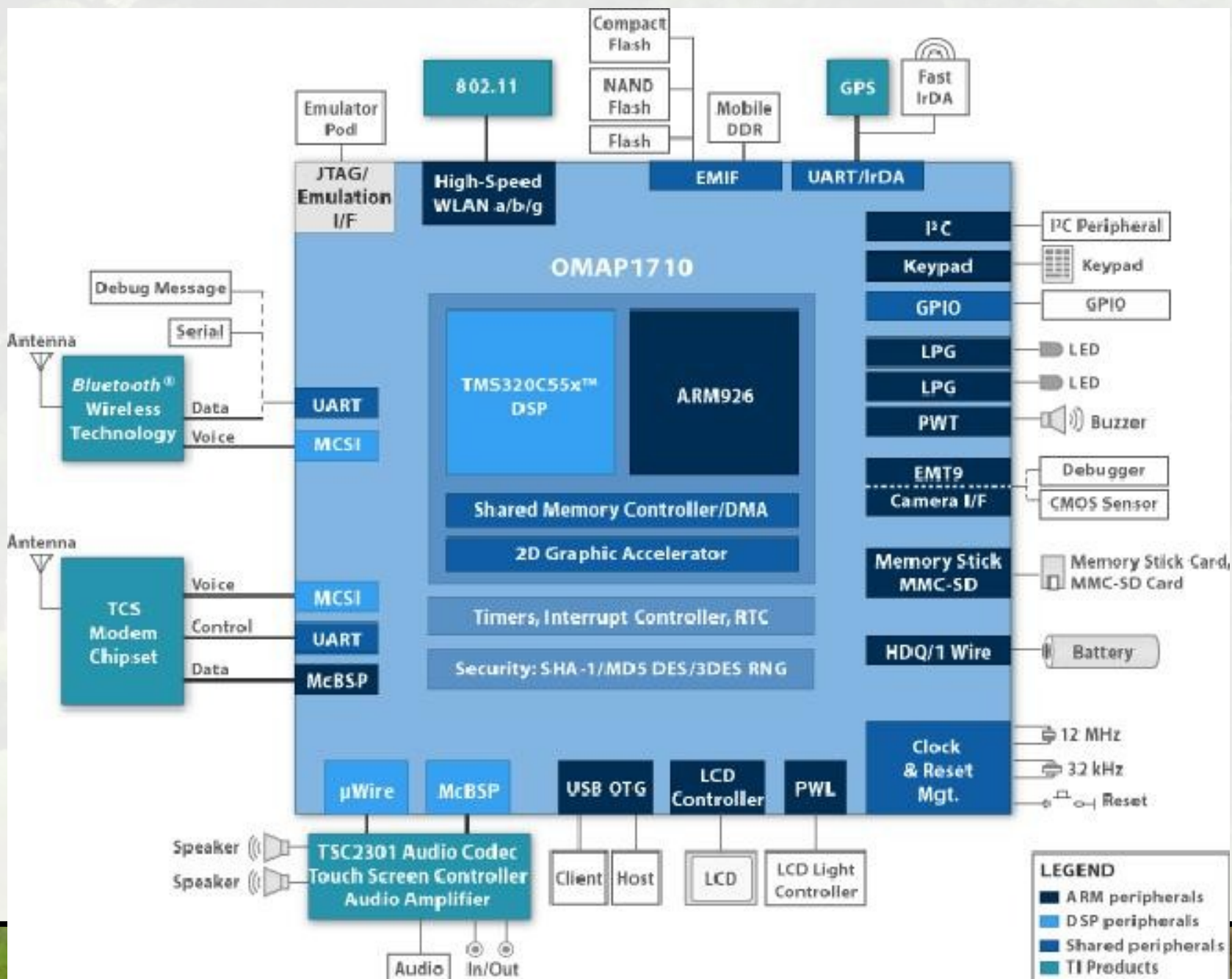
- 2006 年
  - < 200 Million PC sold
  - > 200 Million Phones sold (光第三季)
- 0.5 Billion PC in 2003
- 1.5 Billion consumers own mobile phones worldwide -- Economist, Jan 2006
- 3 Billion subscribers by 2008



# 裝置



# 行動電話的大量系統整合



## 裝置背後的議題 (2)

• 誰在聽你  
講電話？

• 不只是情人間的細語呢喃

# 通訊自由權 (1)

- ? 華民國憲法第二章第七條保障的基本人權
  - 人身自由 (第 8 條)
  - 言論、講學、著作及出版自由 (第 11 條)
  - 秘密通訊自由 (第 12 條)
- 1999 年六月 22 日三讀通過「通訊保障及監察法」
- 依據「電信法」第七條，「秘密通訊」分兩項：
  - 電信之「內容」(監聽)
  - 電信之「有無」(通聯查詢)

# 通訊自由權 (2)

- 「自由、自由，多少罪惡假汝之名而行！」
  - 羅蘭夫人於送上斷頭台前夕
- 通訊法規與法治人權
  - 違反「法律保留原則」
    - 憲法第二十三條之基本原則：通聯之調閱應以法律而非以行政命令來規範
  - 違反「比例原則」
    - 不應以一條街或一個地區為執行之範圍
  - 違反「透明化原則」與「保護隱私權原則」
    - 調閱「通聯」應適用執行「監聽」之規定，於執行結束後應通知受監察之人

# • 封閉的系統

- 壟斷性的電信業者

# 待開放的電信網路 (1)

- 許多廠商與組織指出，電信廠商的限制將阻礙無線網路與電信發展
- Skype
  - 向 FCC 提出請願書，要求立法部門放鬆限制
  - 要求 FCC 為無線網路建立開放標準組織
- openmoko
  - 建構 100% open source 手機
  - 不受電信廠商約束，直接將手機賣給用戶

## 待開放的電信網路 (2)

- 電信廠商僅針對由自家銷售的手機和服務開放網路支援
  - 通常採取封閉技術以鎖定所銷售的手機
- 2007年二月，哥倫比亞大學法學系教授 Tim Wu 於 blog 譴責：
  - 「強勢操控設備和應用市場的產品設計與創新，因而損害消費者的利益」
- 兩大公益組織支持：
  - Public Knowledge
  - Media Access Project (MAP)

- 手機禁用的功能

# 手機禁用的功能

- Wi-Fi (dual-mode phone)
- Bluetooth file transfer (high volume)
- Built-in wireless connectivity CE
- Dialing timer
- Limited to specific network

- 手機受限的功能

# 手機受限的功能

- 某些 GPS 服務應用
- 某些先進的 SMS 功能
- 某些行動瀏覽器
- 基於商業利益的行爲
  - Cingular/AT&T Wireless 曾要求 Nokia 移除歐洲版 E61/62 Smartphone 內的 Wi-Fi，才可在美國網路中使用
  - Verizon 禁止 phone vendor 啟用 bluetooth 檔案傳輸功能，只因爲希望用戶將 camera 所生的照片傳到 (收費的) Verizon 網站
  - ....

# • 手機製造商與應用服務者的訴求

- Skype 於 2007.02.21 向 FCC 提出請願書

# 製造商與應用服務者的訴求 (1)

- 要求電信業者同意
  - 只要不具危險性
    - 任何設備均可連接到其網路
    - 任何應用均可執行於其網路
  - 用戶可瀏覽所有合法的網站
- 成立獨立專注於相關行動應用的產業組織

## 製造商與應用服務者的訴求 (2)

- 是的，我們存活於  
謊言、背信、行為受限、  
受監視、缺乏自由  
的陰影之下
- 部份電信廠商在服務條款中禁止使用 Skype
- Skype 的訴求基本上就是加強 Carterfone 規則

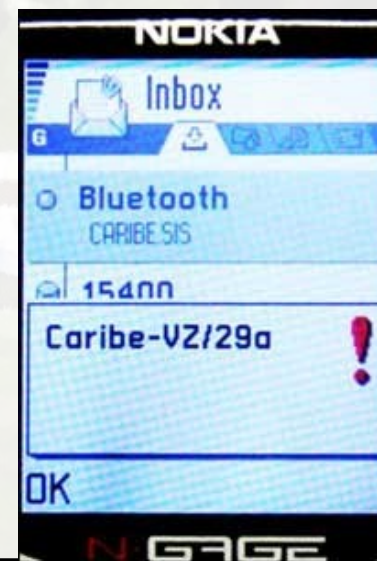
## 安全性挑戰 (1)

# • 第一代

- 手機病毒、蠕蟲、惡意程式

# 典型手機病毒蠕蟲

- Symbian S60, Proof-of-Concept
- PC virus: 1986
- Mobile phone virus/worm: 2004
  - Caribe - Bluetooth
  - Redbrowser – Java-enabled WAP browser
  - Zafi-B – Email/MMS
- 思維
  - 應用程式的漏洞
  - SmartPhone
    - 「它聰明，你傻瓜」



## 安全性挑戰 (2)

# • 第二代





## 第二代：？

- 狄更斯《雙城記》名句：

「那是最美好的  
時代，也是最  
惡劣的時代」

# 第二代手機安全性思維

- SIM Toolkit
- 交叉網路機制 (hand-over)
  - GSM/GPRS/UMTS
  - Wifi
  - 3G/3.5G/HSDPA
- SMS/MMS 的延伸
- RF/Baseband
  - 專屬 AT command 的攻擊方式

# • 第三代？

- SIM card / Telecom / Protocol
- + PC attack stratege
- + Web attack stratege
- + Radius attack

## 安全性挑戰 (4)

- 越 smart  
越 scale



# 結論

- 電信通訊攸關你我生活，眾多的標準、政治性商業考量限制更多元的應用
- 行動通訊與自由
- 普及運算的時代到來
  - 面對前所未有的安全衝擊
- 美國憲法：「人民有免於恐懼的自由」