

# FON：技術簡介

2008 年 2 月

© 香港特別行政區政府

這份文件的內容為香港特別行政區政府的財產，未經香港特別行政區政府的明文批准，不得轉載全部或部份文件內容。

**免責聲明：**政府盡力確保本文資料準確，但不明示或隱含保證資料準確無誤。對於因使用本文資料而引致或與之有關的任何錯誤或遺漏，香港特別行政區政府概不承擔任何法律責任。

## 目錄

摘要.....	2
I. 何謂 FON? .....	3
爭議及趨勢 .....	3
透過 FON WI-FI 網絡連接公司內部網絡.....	4
II. FON 接駁點的基本保安功能 .....	5
III. 潛在的保安威脅 .....	6
無線探取 .....	6
未經授權接達 .....	6
網上攻擊媒介 .....	6
LA FONERA 可能存在的保安漏洞 .....	6
IV. 保安措施 .....	7
更改預設設定 .....	7
採取其它保障措施 .....	7
加強端點保安 .....	7
持續更新接駁點的固件 .....	7

## 摘要

現時電腦用家經常連接到網絡，而網絡及互聯網連接是許多電腦工作不能缺少的。無線網絡已非常普及，不少餐室、機場和許多其它地點也提供無線上網熱點。因無線網絡接達互聯網的技術發展迅速，且廣受歡迎，共用個人家居互聯網連線的想法便出現了。FON Wi-Fi 網絡日漸成為最受歡迎的 Wi-Fi 共用網絡之一。本文將概述 FON Wi-Fi 網絡可能出現的相關保安威脅及可採取的相應保安措施。

## I. 何謂 FON ?

Martin Varsavsky 是一位以西班牙為基地的阿根廷裔企業家。他率先提出透過共用家居或工作場所的個人 Wi-Fi 寬頻連線，達致全球免費使用 Wi-Fi<sup>1</sup>。Martin Varsavsky 其後在英國成立 FON Wireless, Ltd. (或稱「FON」)。FON 旨在建立一個全球 Wi-Fi 社群，成員間彼此共用 Wi-Fi 互聯網連線，把過往互不相干的無線上網熱點改造為一個全球性的 Wi-Fi 群<sup>2</sup>。

根據 FON 的定義<sup>3</sup>，FON 社群是一群 FON 註冊會員。會員分為三類：

1. *Linus*：與FON社群共用帶寬以換取免費連接到任何FON熱點的FON註冊用戶。
2. *Bill*：提供熱點以換取報酬的 FON 註冊用戶。
3. *Alien*：沒有提供FON熱點的註冊用戶，須購買FON通行證後方可使用*Linuses*或*Bills*提供的熱點，以連接到FON社群。

*FONero* 指 FON 社群的 *Linus* 或 *Bill* 會員<sup>4</sup>。

所有 *FONero* 於加入 FON 社群時，須在 FON 網站註冊及開設帳戶<sup>5</sup>。如要與其他 *FONeros* 共用無線互聯網接駁點，*FONero* 須購買 FON Wi-Fi 路由器，如「La Fonera」或「La Fonera+」等<sup>6</sup>。擁有合適的 Wi-Fi 路由器後，只須把 FON Wi-Fi 路由器接駁至寬頻數據機，便可開始與別人共用互聯網帶寬。除此以外，他們亦可選擇在兼容 FON 軟件的路由器上安裝 FON 軟件，藉此與 FON 社群共用寬頻連線。FON 路由器軟件是基於 OpenWRT<sup>7</sup>軟件開發，屬於供嵌入式裝置使用的開放源碼 Linux 發行版。

### 爭議及趨勢

FON 網絡的核心概念是以免費或收取少量費用的方式，與別人共用個人的互聯網帶寬。原則上，這是個好主意，但可能觸犯 *FONero* 所使用的互聯網服務供應商 (ISP) 訂明的條款及條件。當註冊為 *FONero* 時，FON 的條款及條件包括規定註冊人「*have a contract with an ISP that permits the FONero to share bandwidth*」<sup>8</sup>。

---

<sup>1</sup> <http://www.fon.com/en/info/whatsFon>

<sup>2</sup> [http://www.infoworld.com/article/05/12/01/HNhotspotsunite\\_1.html](http://www.infoworld.com/article/05/12/01/HNhotspotsunite_1.html)

<sup>3</sup> [http://static.fon.com/images/media/en/en\\_general\\_conditions.pdf](http://static.fon.com/images/media/en/en_general_conditions.pdf)

<sup>4</sup> [https://static.fon.com/images/media/en/en\\_general\\_conditions.pdf](https://static.fon.com/images/media/en/en_general_conditions.pdf)

<sup>5</sup> <https://www.fon.com/en/register/form>

<sup>6</sup> <http://www.fon.com/en/download#>

<sup>7</sup> <http://openwrt.org/>

<sup>8</sup> [https://static.fon.com/images/media/en/en\\_general\\_conditions.pdf](https://static.fon.com/images/media/en/en_general_conditions.pdf)

然而，FON 已與多家互聯網服務供應商建立夥伴關係。這些互聯網服務供應商願意向其用戶推廣 FON 服務，其中包括英國的 British Telecom<sup>9</sup>、美國的 Time Warner Cable<sup>10</sup>、法國的 Neuf Cegetel<sup>11</sup>等。

### 透過 FON WI-FI 網絡連接公司內部網絡

應避免通過 FON Wi-Fi 網絡連接到公司內部網絡。經 FON Wi-Fi 網絡傳輸的資料可遭附近的人竊取／探取。由於保安控制不足，故在 FON Wi-Fi 網絡傳輸數據並不安全。如果因業務需要而進行連接，有關機構必須採取充分的保安措施，例如以虛擬私有網絡（VPN）把網絡通訊加密及使用多重認證使認證程序更嚴格。

---

9

[http://www.infoworld.com/article/07/10/04/Fons-shared-Wi-Fi-network-goes-mainstream-with-BT\\_1.html](http://www.infoworld.com/article/07/10/04/Fons-shared-Wi-Fi-network-goes-mainstream-with-BT_1.html)

<sup>10</sup> [http://www.infoworld.com/article/07/04/23/HNfonsharesbroadband\\_1.html](http://www.infoworld.com/article/07/04/23/HNfonsharesbroadband_1.html)

<sup>11</sup>

<http://blog.fon.com/en/archive/business/fon-and-neuf-cegetel-begin-rollout-of-new-joint-service.html>

## II. FON 接駁點的基本保安功能

為提供合理的保安及私隱保障水準，FON 接駁點已配備多項基本保安功能：

### 1. 公用及私人服務設定識別碼 (SSIDs)

FON 路由器發出兩種 Wi-Fi 訊號，把寬頻連線分為兩個不同的 Wi-Fi 網絡。兩種訊號分別為公用（預設 SSID 為「FON\_AP」）及私人（預設 SSID 為「MyPlace」）網絡訊號<sup>12</sup>。以「FON\_AP」為 SSID 的無線局部區域網絡 (WLAN) 訊號可供所有 FON 用戶連接，而以「MyPlace」為 SSID 的訊號用作私人網絡，只供 FON 接駁點的擁有人使用。在這個 WLAN 內的所有通訊均已加密處理。每個 FON 接駁點可支援多種無線加密標準，包括有線等效保密規約 (WEP)、WPA 及 WPA2。用戶的私人 WLAN 已利用 FON 裝置的序號作為預先共用密碼匙 (pre-shared key)<sup>13</sup>來預設 WPA 加密的啟用。

### 2. 接達控制

FON Wi-Fi 路由器的固件 (firmware) 是開發自 OpenWRT (基於 GNU/Linux 開發的固件供嵌入式裝置使用)。固件內建接達控制功能，包括一個分隔公用及私人 WLAN 的防火牆。

### 3. 用戶認證及控制

所有 FON 用戶須在註冊後方可使用 FON 網絡。用戶連接到 FON 接駁點時，會被轉導至 FON 的入門網站，經 FON 核實身份後，才可接達網絡。因此，FON Wi-Fi 路由器的擁有人可檢視連接至該接駁點的 FON 用戶名單，並核實透過入門網站連接的 FON 用戶身份。

### 4. 只要 FON Wi-Fi 路由器連接至互聯網，固件便會自動進行更新。

---

<sup>12</sup> [http://static.fon.com/images/media/en/en\\_QIG.pdf](http://static.fon.com/images/media/en/en_QIG.pdf)

<sup>13</sup> <http://www.sbprojects.com/knowledge/internet/fon/index.htm>

### III. 潛在的保安威脅

FON Wi-Fi 網絡為其用戶提供便利，但亦使他們面臨多種保安威脅。下文描述 *FONeros* 參與 FON Wi-Fi 社群時，可能面對的一些保安威脅。

#### 無線探取

FON Wi-Fi 網絡的公用網絡通訊並無加密。由於數據是以純文字的方式傳輸，如果涉及敏感通訊或交易，FON 用戶便可能面臨風險。惡意的 *FONero* 或可使用探取工具從網絡取得密碼及登入名稱等敏感資料。

#### 未經授權接達

FON Wi-Fi 路由器出廠時附有預設密碼（例如：La Fonera 的預設用戶名稱及密碼均為 *admin*）。預設密碼廣為人知，因此如果沒有更改預設密碼，攻擊者或可在未經授權的情況下接達 FON 接駁點，從而危及私人 WLAN 的安全。FON Wi-Fi 路由器直接連接至寬頻路由器，或寬頻路由器所連接的局部區域網絡。如果私人 WLAN 的安全受威脅，則該局部網絡內的所有電腦裝置亦有可能受攻擊。

#### 網上攻擊媒介

雖然 FON Wi-Fi 路由器擁有人可限制其他 FON 用戶所使用的帶寬，以連接到該接駁點，甚至可中斷他們的連線，但擁有人無法控制這些來賓連線時的活動，或會讓計劃發動攻擊的惡意攻擊者有機可乘。

#### LA FONERA 可能存在的保安漏洞

由於 FON 社群日趨普及，最終或會吸引攻擊者的注意，發現其它可能存在的網絡保安漏洞。FON 接駁點亦有可能成為攻擊目標之一。舉例說，於 2006 年，兩名德國的學生在用作設定 La Fonera 路由器的 CGI 腳本中發現漏洞，並透過利用該裝置及進入接駁點的根目錄，成功啟動裝置上的一個 SSH 預設程式。他們亦詳述有關程序，以及提供可開啟 La Fonera 路由器的 Perl 腳本<sup>14</sup>。雖然 FON 已修正有關錯誤，但隨著 FON 社群不斷增長，日後可能發現更多 FON 軟件的保安漏洞。

---

<sup>14</sup> <http://stefans.datenbruch.de/lafonera/>

## IV. 保安措施

整體而言，大部份 FON 用戶為家居用戶。以下列出家居用戶使用 FON Wi-Fi 網絡時應採取的若干保安措施。如果機構有意把其公司網絡連接至 FON 社群，亦應考慮採取這些措施。

### 更改預設設定

由於 FON 接駁點的預設設定（包括管理密碼及 WPA 加密密碼）廣為人知，並可輕易取得，因此建議立即更改預設設定，以防止別人在未經授權的情況下接達 FON 接駁點。

### 採取其它保安措施

由於私人 WLAN 與家居網絡之間的連接不設接達控制，因此當私人 WLAN 的安全受威脅時，並無足夠的保護措施以保護家居網絡的個人電腦免受外來攻擊。因此，應在連接於家居網絡的所有電腦裝置安裝防火牆，以抵禦可能來自私人 WLAN 的攻擊。

### 加強端點保安

FON Wi-Fi 網絡是由 FON 社群成員擁有及控制的私人 WLAN 所組成，可視為合作性的熱點網絡。原則上，用戶應視 FON Wi-Fi 網絡為不可靠的網絡，而流動裝置在連接到任何 FON Wi-Fi 網絡前，應安裝和運行充足的保安措施（如安裝防毒軟件、最新的保安修補程式及個人防火牆）。

應採用加密技術保護儲存於流動裝置的個人資料和敏感資訊，以及為連接至公司伺服器的通訊或其它交易服務提供保障。

### 持續更新接駁點的固件

無線網絡接駁點製造商不時就其生產的裝置發放固件更新或修正程式。接駁點必須時常安裝最新的修正程式。至於 FONero 擁有的 La Fonera 路由器，應確保 FON 提供的自動固件更新功能操作正常。