

FON: A TECHNOLOGY BRIEF

February 2008

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary	2
I. What is FON?	3
Issues and Trends	4
Connecting To a Corporate Internal Network Through Fon Wi-Fi Network	5
II. Basic Security Features of FON Access Points	6
III. Possible Security Threats	8
Wireless Sniffing	8
Unauthorised Access	8
Cyber Attack Vehicle	9
Possible Security Flaws in La Fonera	9
IV. Security Measures	10
Change the Default Settings	10
Implement Additional Safeguards	10
Enhance Endpoint Security	11
Keep Access Points Patched	11

SUMMARY

Network connectivity is now a ubiquitous part of the computing experience. Network and Internet connectivity are vital in so many computing tasks today. In terms of access to networks, wireless connectivity has gained in popularity, and wireless hotspots can now be found in cafes, airports, and many other locations. Due to the tremendous growth and popularity of wireless Internet access, the idea of sharing one's home Internet connection has come about. The FON Wi-Fi network is becoming one of most popular Wi-Fi sharing networks. In this paper, we provide a brief discussion of the FON Wi-Fi network, related possible security threats and corresponding security measures that can be taken.

I. WHAT IS FON?

The idea of making Wi-Fi universal and free¹ by sharing individual Wi-Fi broadband access from home or work was first introduced by Martin Varsavsky, an Argentinian entrepreneur based in Spain. Varsavsky later founded the company FON Wireless, Ltd. (or “FON”) in the UK. FON aims to build a global Wi-Fi community of people sharing and using each other's Wi-Fi Internet connections, creating a global Wi-Fi “cloud” out of what used to be disparate hotspots².

As defined by FON³, a FON community is a group of members registered with FON, that has three categories of membership:

1. *Linus* is a registered user of FON who shares bandwidth with the FON community in exchange for free connection to any FON hotspot.
2. *Bill* is a registered user of FON who offers a hotspot in exchange for compensation.
3. *Alien* is a registered user who does not offer a FON hotspot and who connects to the FON community using the hotspots of *Linuses* or *Bills* after purchasing a FON pass.

The term *FONero* refers to either a Linus or Bill member of the FON community⁴.

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

² http://www.infoworld.com/article/05/12/01/HNhotspotsunite_1.html

³ https://static.fon.com/images/media/en/en_general_conditions.pdf

⁴ Same as above.

All *FONeros* are required to set up and register an account on FON's website⁵ when first joining the FON community. To share a wireless Internet access point with other *FONeros*, a *FONero* needs to purchase a FON Wi-Fi router, such as "La Fonera" or La Fonera+⁶. Once he or she has the Wi-Fi router, they can start sharing their Internet bandwidth with others by simply connecting the FON Wi-Fi router to a broadband modem. Alternatively, they can install FON software onto a FON-compatible router to share their broadband connection with the FON community. Software for FON routers is based on an open-source Linux distribution for embedded devices called OpenWRT⁷.

ISSUES AND TRENDS

The core idea of the FON network is to share one's Internet bandwidth with others either free of charge or for a small fee. This may be a good idea in principle, but it may breach the terms and conditions of the Internet Service Provider (ISP) used by the *FONero*. When a person registers to be a *FONero*, one of the requirements in FON's Terms and Conditions is that the registrant "*have a contract with an ISP that permits the FONero to share bandwidth*"⁸.

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

⁶ <http://www.fon.com/en/download#>

⁷ <http://openwrt.org/>

⁸ https://static.fon.com/images/media/en/en_general_conditions.pdf

FON has, however, established partnership relationships with a number of ISPs who are willing to promote the FON Service to their subscribers. Examples are British Telecom⁹ in UK, Time Warner Cable¹⁰ in US, Neuf Cegetel¹¹ in France, and so on.

CONNECTING TO A CORPORATE INTERNAL NETWORK THROUGH FON WI-FI NETWORK

Any connection to a corporate internal network via a FON Wi-Fi network should be avoided. Information transmitted over a FON Wi-Fi network can potentially be tapped or sniffed by others in the area. Data over a FON Wi-Fi network is considered insecure owing to the lack of security controls. If there is really a business need for such connections, organisations should implement sufficient security measures such as deploying a Virtual Private Network (VPN) to encrypt network traffic, and using multi-factor authentication to strengthen the authentication process.

⁹ http://www.infoworld.com/article/07/10/04/Fons-shared-Wi-Fi-network-goes-mainstream-with-BT_1.html

¹⁰ http://www.infoworld.com/article/07/04/23/HNfonsharesbroadband_1.html

¹¹ <http://blog.fon.com/en/archive/business/fon-and-neuf-cegetel-begin-rollout-of-new-joint-service.html>

II. BASIC SECURITY FEATURES OF FON ACCESS POINTS

To provide a reasonable level of security and privacy, a number of basic security features are implemented in FON access points:

1. Public and Private Service Set Identifiers (SSIDs)

A FON router splits a broadband connection into two separate Wi-Fi networks by sending out two Wi-Fi signals: a public one (with SSID “FON_AP” by default) and a private one (with SSID “MyPlace” by default)¹². The WLAN signal with SSID "FON_AP" can be connected to by all FON users, while the signal with SSID "MyPlace" is private and exclusive to the owner of the FON access point. All traffic within this WLAN is encrypted. Each FON access point supports several wireless encryption standards including WEP, WPA, and WPA2. By default, WPA encryption is enabled for the user’s private WLAN, using the device's serial number as a pre-shared key¹³.

2. Access Control

The firmware in a FON Wi-Fi router is developed from OpenWRT, a GNU/Linux based firmware for embedded devices. Access control features, including a firewall, are built into the firmware. The firewall stands between the public and private WLANs.

3. User Authentication and Control

All FON users are required to register to make use of the FON network. During the process of connecting to a FON access point, a user is redirected

¹² http://static.fon.com/images/media/en/en_QIG.pdf

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

to FON's access portal and is required to authenticate with FON before gaining access to the network. As a result, the owner of a FON Wi-Fi router is able to view a list of FON users connected to his access point and verify the identities of FON users connected through the access portal.

4. Firmware updates to the FON Wi-Fi router are done automatically, provided that it is online.

III. POSSIBLE SECURITY THREATS

A FON Wi-Fi network may provide convenience to its participants, but it may also expose users to a number of security threats. The following section describes some of the security threats *FONeros* may face when participating in the FON Wi-Fi community.

WIRELESS SNIFFING

Public traffic on a FON Wi-Fi network is not encrypted. This can put FON users at risk if sensitive communications or transactions are involved, because the data is being transmitted as plaintext. A malicious *FONero* might be able to use sniffing tools to obtain sensitive information such as passwords and login IDs from the network.

UNAUTHORISED ACCESS

A FON Wi-Fi router is shipped with a default password (e.g. the default username and password of La Fonera are both *admin*). The default passwords are widely known and attackers might be able to gain unauthorised access to a FON access point, compromising the security of the private WLAN if the default passwords have not been changed. The FON Wi-Fi router is directly connected to a broadband router, or to a local area network where a broadband router is attached. If the private WLAN is compromised, the machines on the local network will also be open to attack.

CYBER ATTACK VEHICLE

Although the owner of a FON Wi-Fi router can limit the bandwidth used by other FON users connected to the access point, and can even terminate their connections, the owner has no control on the activities of his guests when they are online. This may provide good cover for malicious attackers planning on launching attacks.

POSSIBLE SECURITY FLAWS IN LA FONERA

Due to the growing popularity of the FON community, this may eventually attract the attention of attackers who could uncover other possible security flaws in the network. One of the possible targets is a FON access point. For example in 2006, two students from Germany discovered vulnerabilities in the CGI scripts used to configure the La Fonera router, successfully activating an SSH daemon on the device by exploiting the device and gaining root access to the access point. They also provided a detailed description of the procedure and ready-to-use Perl scripts to open up a La Fonera¹⁴. Although FON has now fixed this bug, more vulnerabilities in FON software could emerge as the FON community grows.

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

IV. SECURITY MEASURES

On the whole, most FON users will be home users. The following are some security measures that home users should employ when using a FON Wi-Fi network. If an organisation really wants to attach its corporate network to a FON community, the same security measures should be considered.

CHANGE THE DEFAULT SETTINGS

Because the default settings in a FON access point, such as the administrative password and WPA encryption key, are well known or can be obtained without any difficulty, it is recommended the default settings be changed immediately to protect unauthorised access to the FON access point.

IMPLEMENT ADDITIONAL SAFEGUARDS

As there is no access control between the private WLAN and a home network, there is no adequate protection in place to protect PCs on the home network from an attack launched from outside if the private WLAN is compromised. Therefore, a personal firewall should be installed on all machines running within the home network to guard against potential attacks originating from the private WLAN.

ENHANCE ENDPOINT SECURITY

The FON Wi-Fi network is built with WLANs owned and controlled by members of the FON community. The network can be viewed as a cooperative hotspot network. As a rule of thumb, users should consider the FON Wi-Fi network to be an un-trusted network, and adequate safeguards (such as installation of anti-virus software, updated security patches and personal firewalls) should be installed and running on mobile devices before connecting to any FON Wi-Fi network.

Encryption technologies should be used to protect personal data and sensitive information stored in mobile devices as well as across communication connections to company servers or other transactional services.

KEEP ACCESS POINTS PATCHED

From time to time, the manufacturers of wireless access points release firmware updates or fixes for their devices. It is necessary to keep access points patched with the latest fixes. Ensure the automatic firmware update from FON is working properly on all La Fonera routers owned by the *FONero*.