

A **Shimon Systems** White Paper



2870 Zanker Road, Suite 100  
San Jose, CA 95134  
408-546-2140  
[www.shimonsystems.com](http://www.shimonsystems.com)

## **Bio-NetGuard (v 2.x): Fingerprint-based Wireless LAN Access Control**

- *Gurminder Singh*  
CTO  
[gurminder@shimonsystems.com](mailto:gurminder@shimonsystems.com)

November 17, 2006

## Contents

---

<b>Introduction</b> .....	<b>3</b>
<b>WiFi LAN Technologies</b> .....	<b>3</b>
WiFi Security Vulnerabilities .....	4
Security Solutions in WiFi LANs .....	5
<b>Biometrics</b> .....	<b>5</b>
<b>Bio-NetGuard™: Fingerprint-based WiFi LAN Access Control</b> .....	<b>6</b>
Robust Multifactor Security.....	7
Plug-and-Play Design .....	7
Fully Contained Device .....	7
<b>Bio-NetGuard Architecture</b> .....	<b>7</b>
<b>Bio-NetGuard Architecture</b> .....	<b>8</b>
Support for Roaming .....	9
Multifactor Authentication.....	10
<b>Bio-NetGuard: Making it work in the Enterprise</b> .....	<b>10</b>
<b>Bio-NetGuard: Comparison with Other Solutions</b> .....	<b>11</b>
<b>Summary</b> .....	<b>11</b>



## Introduction

In recent years, there has been an explosive growth in the use of WiFi local area networks (WLANs). This is a direct result of the tremendous convenience and cost savings offered by WiFi. While the use of WiFi has grown rapidly, there are serious concerns about its security. One such concern is that unauthorized users are able to connect to the network and misuse enterprise resources. Due to such concerns, many enterprises either use the technology reluctantly or have postponed its use until its security issues are adequately addressed.

Biometrics has been attracting significant attention to help solve some of the security problems in information systems. Biometric technologies enable the identification of users based on their physical and/or behavioral characteristics, such as fingerprint, facial features and voice pattern. Among the various biometric technologies, the use of fingerprint has become the most popular. Fingerprint technology is a cost-effective, robust and convenient technology to use for user identification and verification.

Bio-NetGuard provides fingerprint-based access control to the enterprise WLAN at the very first point of contact to the network—the WiFi Access Point. By combining the

latest WiFi security and biometric identity verification technologies, Bio-NetGuard provides a rock solid access control mechanism for the enterprise network. Before a user can connect to the WLAN, his or her fingerprints must be authenticated by Bio-NetGuard.

Bio-NetGuard is a DSP-based, fully-contained network authentication device that works with any Wireless Protected Access (WPA) compliant access point. It is equipped with its own storage, processor and memory to handle the entire authentication process in a rapid response mode. All user fingerprints and activity logs are maintained on Bio-NetGuard itself. Bio-NetGuard communicates with its clients in a secure mode.

## WiFi LAN Technologies

WiFi (or Wi-Fi), short for Wireless Fidelity, refers to technologies that conform to the IEEE 802.11 family of standards. The term “WiFi” has been promulgated by Wi-Fi Alliance (<http://wi-fi.org/>) which tests and approves technologies to be “Wi-Fi Certified”. WiFi certified products from different manufacturers are expected to interoperate. IEEE 802.11 is a specification for wireless connectivity within a local area network and covers a number of standards including IEEE 802.11a, 802.11b and 802.11g.

Both 802.11b and 802.11g operate in the 2.4GHz band but use different modulation and encoding schemes, whereas 802.11a operates in the 5GHz frequency. Both 802.11a and 802.11g can achieve up to



55mbps whereas 802.11b is limited to 11mbps. Currently, to be cost effective and to provide backwards compatibility, most of the 802.11-compliant equipment conforms to multiple of 802.11a, b and g standards.

WLAN is one of the most rapidly and widely accepted technology in recent years. There are several reasons for its rapid acceptance: reduced cost, reduced time for deployment, support for mobility, and good scaling up properties. Not only is the WLAN equipment low-cost, the use of WLAN eliminates the need for expensive wiring or rewiring of buildings. Directly linked with the elimination of wiring is the time to deploy the WLAN. As a result, WLANs are quickly deployed and immediately accessible to the users. This is one of the significant benefits for new businesses. Furthermore, because WLANs support mobility, users are not tied to a particular location; they are free to move around in the WLAN area of the coverage. Lastly, WLANs offer good scaling properties, often without requiring additional infrastructure. So a small business can grow and yet continue to use the same WLAN. Because of these significant benefits, the WLAN technology has been rapidly accepted by users. This has helped bring down the cost of the technology, further fueling its demand.

Given the benefits of the WLAN technology, it has become popular with many different market segments including enterprise, home, military and first-responders. Different advantages of WLANs appeal to different market segments but each can find compelling reasons to use WLANs.

Despite its success, there are serious concerns about the security of WLANs. As a result, many enterprises either use the technology reluctantly or have postponed its use until its security issues are adequately addressed. The following section provides an introduction to the security vulnerabilities of WiFi.

#### *WiFi Security Vulnerabilities*

When compared to wired LANs, WLANs suffer from an inherent problem: since the WLAN signal is broadcast, it is available to everyone in the radio range. In wired LANs, people need to physically connect to the wire to receive the signal. In WLANs however, anyone who can receive the WLAN signal can intercept the signal and eavesdrop. This is a serious vulnerability as any data the user is transmitting or receiving can potentially be viewed or worse changed by an intruder.

In wired LANs, the need to physically connect to the wire prevents unauthorized access to the network. No such restriction exists in WLANs. WLAN access points broadcast their signal and receive signals from users in their radio range. So anyone who can get hold of the information to connect to the network can connect.



In addition to the above, WLANs are exposed to Denial of Service (DoS) attacks. Since WLANs do not have a well defined boundary, a malicious station can launch an attack in order to stop legitimate communication.

#### *Security Solutions in WiFi LANs*

WEP, short for Wired Equivalent Privacy, is intended as a scheme to provide the same level of security in WLANs as that of a wired LAN. The basic idea in WEP is to encrypt data using a combination of user-defined and automatically generated keys. WEP is symmetric in nature which means that the same key that is used for encrypting the transmitted data is also used for decrypting it upon receipt. A number of flaws have been discovered in the WEP algorithm and its implementation, which seriously undermine the security claims of the system. Programs to automatically find keys of WLANs are readily available on the Internet. As a result WEP is no longer considered a significant way of protecting enterprise networks.

WEP encrypts data and tries to make it obscure to eavesdroppers, but it does not prevent unauthorized computers from connecting to WLANs. MAC (Media Access Control) address filtering deals with this issue. The system administrators can enter the MAC addresses of authorized computers in the access

point. The access point from then on allows only those computers (or NICs to be more precise) which have the authorized MAC address. Any addresses not explicitly defined in the filter are denied access. While the idea of MAC address filtering has some merit, it is unfortunately not very secure. It is rather easy to spoof MAC addresses and hence gain access to the WLAN. Another problem with MAC address filtering is that it authenticates the equipment rather than the user.

The IEEE 802.11i standard has been developed to address the security vulnerabilities of WLANs and supercedes WEP and WPA, an intermediate solution to WEP insecurities developed by the Wi-Fi Alliance. 802.11i uses IEEE 802.1X for authentication, RSN (Robust Security Network) for keeping track of associations and AES-based encryption to provide confidentiality, integrity and origin authentication. 802.1X provides authentication to devices attached to a LAN port supporting a point-to-point connection. 802.11i was ratified in June 2004 and is rather comprehensive in its coverage.

#### **Biometrics**

Biometrics refers to the identification of a person based on his or her physical characteristics and/or behavior. Common biometrics include fingerprint, voice pattern, retinal pattern and facial features. Among this large variety of biometric possibilities, the use of fingerprint for identification and verification dominates the market. There are many reasons for this including the low-



cost, high-reliability and fast-response of the fingerprint technology and systems.

The use of fingerprint for user authentication has been on the rise as people have discovered many problems with password and token-based systems. In the last few years, the number of online accounts each user has increased many fold. It is not uncommon for people to have 15 online accounts, and remembering this many passwords is not an easy task, especially for accounts which are accessed infrequently. To solve this problem people end-up writing their account information on paper which is very dangerous as they are prone to misplace or lose it. The difficulty in managing many passwords also results in increasing number of calls to the IT support departments to reset passwords. A similar problem occurs with hardware tokens for authentication. People end-up with many tokens, one for each account, so they are difficult to carry and manage. In addition, it is easy to lose hardware tokens.

Fingerprint-based authentication provides a rather elegant solution to all of the problems associated with passwords and hardware tokens. Since fingerprint technology has become affordable and reliable, its use in user authentication is on a rapid rise. Password Freedom™

from Shimon Systems does a rather elegant job of using fingerprints for logical access control.

### **Bio-NetGuard™: Fingerprint-based WiFi LAN Access Control**

Bio-NetGuard™ provides effective access control for WLANs. Enterprises have been concerned about the weak access control in WLANs. Verifying the identity of the equipment—not the user—has been considered unsafe for any security conscious enterprise environment. Bio-NetGuard is the only effective solution for this problem.

Bio-NetGuard provides Fingerprint-based access control to the enterprise network at the very first point of contact to the network—the WiFi Access Point. By combining the latest WiFi security and biometric identity verification technologies, Bio-NetGuard provides a rock solid access control mechanism for your enterprise network. Before a user can connect to the WiFi LAN, his or her fingerprints must be authenticated by Bio-NetGuard.

Bio-NetGuard is a DSP-based, fully-contained network authentication device that works with any WPA-compliant access point. It is equipped with its own storage, processor and memory to handle the entire authentication process in a rapid response mode. All user fingerprints and activity logs are maintained on Bio-NetGuard itself. Bio-NetGuard communicates with the clients in a secure mode.



Bio-NetGuard can work with all of the popular commercial-off-the-shelf WiFi access points, adapter cards and fingerprint scanners. It takes under 5 minutes to connect and configure Bio-NetGuard in the enterprise network.

### *Robust Multifactor Security*

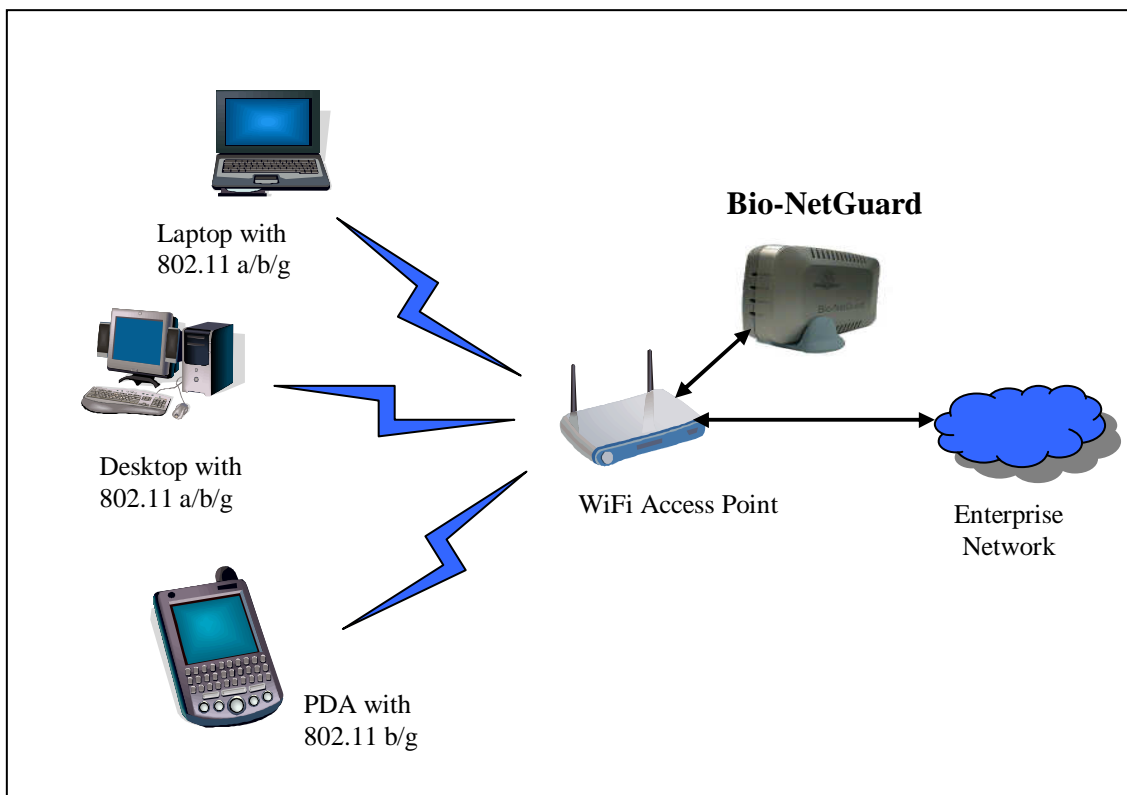
By using fingerprint-based access control, Bio-NetGuard eliminates the vulnerabilities associated with simple MAC filtering and user-id/password access controls. It can optionally provide multifactor – fingerprint and password - authentication.

### *Plug-and-Play Design*

Bio-NetGuard works in a plug and play mode and takes under 5 minutes to install and configure on the network. It is fully compliant with existing and emerging standards for WLAN security and works with a number of commercial-off-the-shelf access points and adapter cards.

### *Fully Contained Device*

Bio-NetGuard is a DSP-based device with its own processor, storage and RAM. Since it does not run any of the standard operating systems, it is virtually hacker-proof.





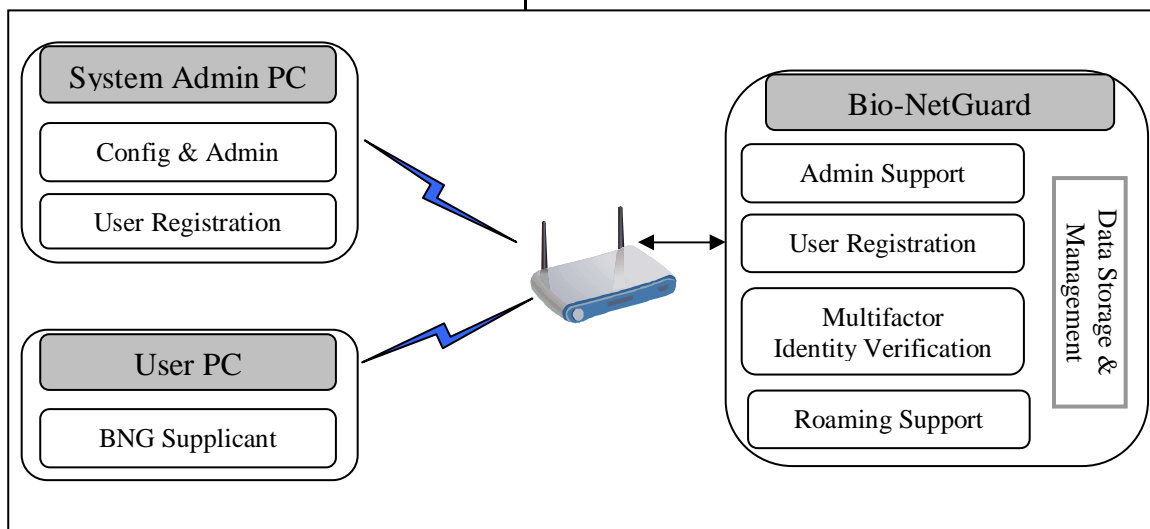
### Bio-NetGuard Architecture

The complete Bio-NetGuard system comprises of the Bio-NetGuard device and the associated software. There are three main components of the software: Bio-NetGuard configuration and administration, user registration, and WiFi supplicant which uses fingerprint-based authentication. Each of these components is distributed in two parts: one part works on the PC and the other corresponding part on the Bio-NetGuard device.

The main function of the Administration software is to enable the system administrator to configure the Bio-NetGuard device with appropriate IP and port numbers and necessary secrets. In addition, the system administrator can view status of user registration and all of the activity taking place on the Bio-NetGuard device.

Once Bio-NetGuard has been configured and added to the enterprise network, the next step is to register user fingerprints. This is achieved by using the Bio-NetGuard user registration program. This program enables the system administrator to register user ids, fingerprints, status (normal or administrator) and expiration date. Once a user has been registered, he or she is allowed to connect to the WiFi access point. Only those users who are registered in Bio-NetGuard are allowed to connect to the network.

When a user tries to connect to a Bio-NetGuard-enabled access point, he needs to provide his user id and fingerprint for authentication. This step is achieved by using the Bio-NetGuard supplicant. This supplicant runs on the user PC, collects the required data from the user and sends it to the WiFi access point which in turn communicates with the Bio-NetGuard device for authentication.





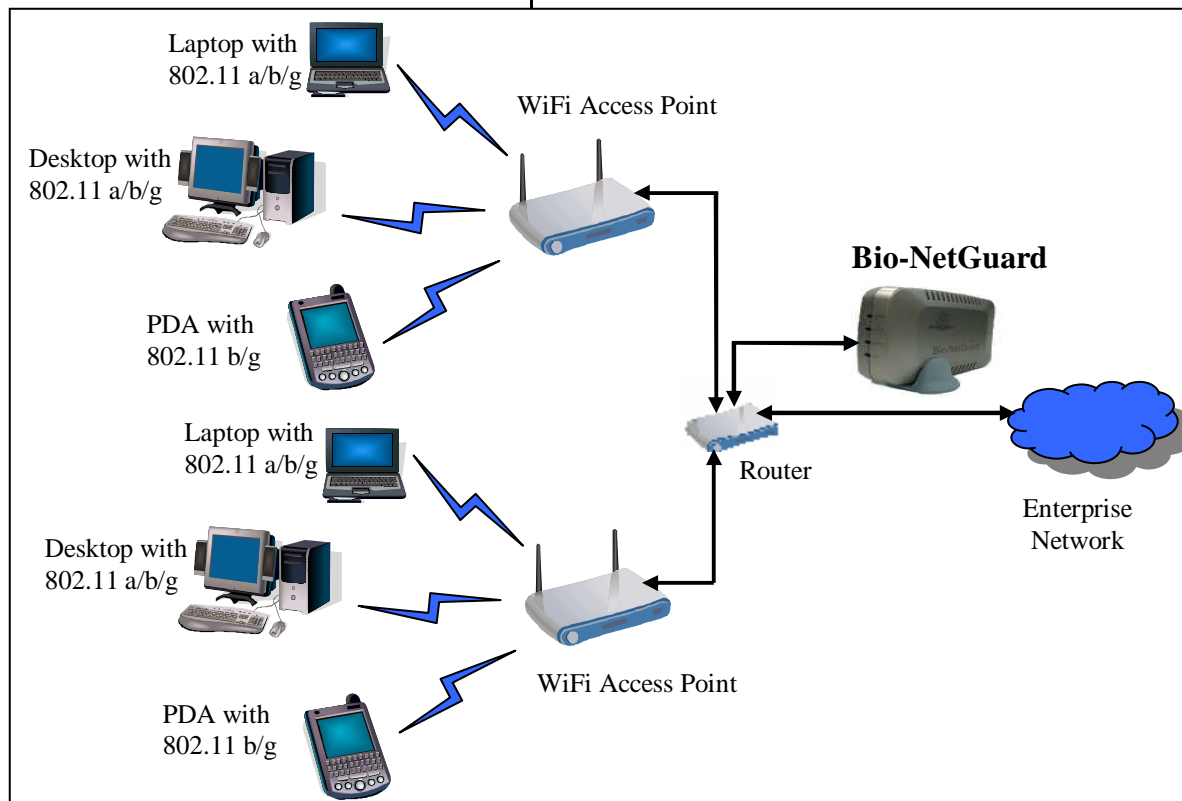
### *Support for Roaming*

Roaming is defined as the transparent re-authentication of the user from one access point to another in a network comprised of multiple access points, one Bio-NetGuard, and a router/DHCP server.

Basic to our implementation of roaming is the concept of the network list. This list contains the SSID and MAC address of every access point on the network where roaming is to occur. No roaming occurs to access points not in the list.

The roaming list is originally created by the administrator using the administration software. This list is given to the Bio-NetGuard with an assigned version number, controlled by the administration software.

When the Bio-NetGuard Supplicant sends its first packet to the Bio-NetGuard (actually the access point, which forwards it to Bio-NetGuard), the packet contains the version number of the list it has. If the version Bio-NetGuard has is different, it will send its roaming list to the Supplicant and the Supplicant will use that list and store the list in a file. The Supplicant uses that roaming list until the list version changes.





Also, since the handoff must be transparent, the user credentials are cached from the original authentication and reused for every handoff. There are no further user authentication requirements.

### *Multifactor Authentication*

Bio-NetGuard supports fingerprint and password authentication types for flexibility and for extra level of security, where needed. A single Bio-NetGuard unit can authenticate users based on their fingerprint only, fingerprint and password, and password only.

The type of authentication a user will use to connect to the network is decided at the time of user registration in Bio-NetGuard. The system administrator will select the right type of authentication technique for the user and collect the appropriate data from the user. Once registered, the user must use the same technique for authentication when connecting to the network.

### **Bio-NetGuard: Making it work in the Enterprise**

Bio-NetGuard helps protect the enterprise network at the first point of contact to the network – the access point. Any 802.11i or WPA2.0 compliant WiFi access point can be easily configured to communicate with Bio-NetGuard quickly and easily. The configuration

requires entering the IP and port numbers of BNG as well as a shared secret between BNG and the access point(s). The entire process of connecting BNG to the network and configuring access point takes under 5 minutes!

When there are multiple access points and the network needs to support roaming among these access points, the administrator creates a list of these access points and enters it in the Bio-NetGuard controlling the access points.

Once BNG has been included in the network, the next step is to register users in BNG. This step is best executed by the system administrator of the enterprise and requires capturing users' fingerprints and/or passwords, as the case maybe, for storage in BNG. Per user it takes under 3 minutes to register their fingerprints. As described in the Bio-NetGuard architecture, it comes equipped with a program to register users. Only those users who have been registered in BNG are able to connect to the access point and hence the enterprise network.

Each user computer needs to have BNG supplicant software. When connecting to a BNG-protected access point, the user provides his fingerprint and/or password depending on the user's registered authentication type. The access point seeks user identity verification from BNG before it grants permission to connect to the access point.



### **Bio-NetGuard: Comparison with Other Solutions**

WLAN security has been an important concern for enterprises. It has been realized that schemes such as WEP and MAC filtering are not robust enough for enterprise use. As a result, enterprises have started to adapt existing solutions to make their networks more secure. Prominent among them are the use of virtual private networks (VPNs) and user-name password authentication servers.

In using a VPN, an enterprise WLAN is treated at the same level of security (or insecurity) as an external network, i.e., users are made to follow the same procedure that they would if they were connecting to the enterprise from an external network. There are a number of issues with this approach including the extra cost of setting-up and administering the enterprise VPN and inconvenience of having to go through the VPN process even when the user is located on site at the enterprise!

The second option is to use standard user-id/password authentication which is used for logical access control in the enterprise. This way of access control for WLANs is rather expensive to install, maintain and administer. It is well-known how cumbersome it is to manage such systems. Additionally, this approach

is fraught with all of the problems associated with using user-id/password for user identity.

Bio-NetGuard provides significant cost and operational advantages over both these approaches. By providing a fully-contained, plug-and-play, and robust solution, it eliminates the need to devote expensive hardware and software as well as cumbersome management of the system. Not only does BNG reduce cost and management overhead, it provides a level of security which goes far beyond what is offered by other approaches.

### **Summary**

Bio-NetGuard enables rock-solid security in WiFi LANs by authorizing connections to the WiFi LAN based on user fingerprints and/or passwords. By doing so Bio-NetGuard goes far beyond any of the existing WiFi security products. Bio-NetGuard is a DSP-based, fully-contained unit with its own processor, memory and storage. All user data and logs are maintained and all processing is done on Bio-NetGuard itself. This makes the device easy to install, configure and maintain. Bio-NetGuard supports roaming across a mix of different vendors' access points. A single Bio-NetGuard unit can support a variable number of access points. Bio-NetGuard does not use any of the standard operating systems, making it virtually hacker-proof! Bio-NetGuard is the only device in market providing this level of security for enterprise WiFi LANs.