## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>2</td>
</tr>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Security Concerns in WiFi LAN</td>
<td>3</td>
</tr>
<tr>
<td>WiFi Security Vulnerabilities</td>
<td>4</td>
</tr>
<tr>
<td>Security Solutions in WiFi-LANs</td>
<td>4</td>
</tr>
<tr>
<td>Advantage of Biometrics for Security</td>
<td>5</td>
</tr>
<tr>
<td>SECURED BioNet™: The Fingerprint-based WiFi LAN Security Solution</td>
<td>5</td>
</tr>
<tr>
<td>Robust Security</td>
<td>6</td>
</tr>
<tr>
<td>Plug-and-Play Design</td>
<td>7</td>
</tr>
<tr>
<td>Hacker Proof Device</td>
<td>7</td>
</tr>
<tr>
<td>SECURED BioNet Architecture</td>
<td>7</td>
</tr>
<tr>
<td>SECURED BioNet is Easy To Deploy</td>
<td>8</td>
</tr>
<tr>
<td>Comparison of SECURED BioNet with Other Solutions</td>
<td>8</td>
</tr>
<tr>
<td>Summary</td>
<td>9</td>
</tr>
</tbody>
</table>
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 unauthorized users being 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.

SECURED BioNet™ 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, SECURED BioNet 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 SECURED BioNet.

SECURED BioNet 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 the SECURED BioNet device itself. SECURED BioNet communicates with its clients (wireless access points) in a secure mode.

Security Concerns in WiFi LAN

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.

Given the benefits of the WLAN technology, it has become popular with many different market segments including enterprise, home, military and various mobile workforce situations.

Despite its success, there are serious concerns about the security of WLANs. 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. As the WLAN signal is broadcast, it is available to everyone in the radio range. In wired LANs, people need to physically connect to the network 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. 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 a scheme intended to provide the same level of security in WLANs as that of wired LANs. The basic idea of 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 that 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. MAC (Media Access Control) is a hardware address that uniquely identifies each node of a network. The system administrator can enter the MAC addresses of authorized computers in the Wireless access point. The access point would only allow only those computers (or NICs to be more precise) which have the authorized MAC address to access the WLAN. 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. The other 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. WPA is 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
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.

**Advantage of Biometrics for Security**

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 used by each person has increased. It is not uncommon for people to have 15 online accounts. The task of remembering many passwords is not an easy task, especially for accounts which are accessed infrequently. In order to solve this problem, people often write their account information on paper. This practice is very dangerous as many are prone to misplace or lose it. The difficulty in managing many passwords also results in an increased number of calls to the IT department for password related issues. A similar problem occurs with hardware tokens for authentication. People often end up with tokens for each account, so they become 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 the rise. A related product to SECURED BioNet from SutiSoft does a rather elegant job of authenticating fingerprints for logical access control to applications and enterprise networks. This product is usable in places where there is no wireless network in use.

**SECURED BioNet™: The Fingerprint-based WiFi LAN Security Solution**

SECURED BioNet 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, SECURED BioNet 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 SECURED BioNet.

SECURED BioNet is a DSP-based special purpose hardware 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 SECURED BioNet device itself. SECURED BioNet communicates
with the clients (the access points) in a secure mode.

The administration utilities provided with SECURED BioNet also allow the system administrator to back up and restore the userid and user credentials that are stored on the SECURED BioNet device over to a server or storage device. The system administrator utility also allows the merging of user credentials when combining two SECURED BioNet devices into a single device or for reconfiguration purposes.

**Robust Security**
SECURED BioNet provides a way of providing robust and intrusion proof security for WLANs. By using fingerprint-based access control, it eliminates the vulnerabilities associated with simple MAC filtering and user-id/password type access controls.
**Plug-and-Play Design**
SECURED BioNet works in an easy plug and play manner and comes with its associated software. It takes under five minutes to install and configure the system. 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.

**Hacker Proof Device**
SECURED BioNet 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.

**SECURED BioNet Architecture**
The complete SECURED BioNet system is made up of the SECURED BioNet device and the associated software. There are three main components of the software: SECURED BioNet configuration and administration, user registration, and WiFi supplicant (client) software 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 SECURED BioNet device.

The main function of the Administration software is to enable the system administrator to configure the SECURED BioNet 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 SECURED BioNet device.
Once SECURED BioNet has been configured and added to the enterprise network, the next step is to register user fingerprints. This is achieved by using the SECURED BioNet user registration program. This program enables the system administrator to register user ids, fingerprints, privilege (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 SECURED BioNet device are allowed to connect to the network.

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

SECURED BioNet is Easy To Deploy
SECURED BioNet is architected to be easily and incrementally deployed in an enterprise. As capacity requirements increase, it is possible to add more SECURED BioNet devices to your already existing wireless access points. The plug and play architecture of the system with easily configurable software enables easy installation without much system knowledge by the user.

Comparison of SECURED BioNet with Other Solutions
WLAN security is of utmost importance for enterprises. Security methods such as WEP and MAC filtering are not robust enough for enterprise use. As a result, enterprises have implemented alternative solutions to make their networks more secure. Prominent among them being the use of virtual private networks (VPNs) and user-name password authentication servers.

With a VPN setup, an enterprise WLAN is provided only 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 authentication.

SECURED BioNet 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 the cumbersome management of the VPN system. Not only does BioNet reduce cost and management overhead, it provides a level of security which goes far beyond what is offered by other approaches.

Summary
SECURED BioNet enables rock-solid security in WiFi LANs by authorizing connections to the WiFi LAN based on user fingerprints. SECURED BioNet goes far beyond any of the existing WiFi security products.

SECURED BioNet 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 SECURED BioNet itself. This makes the device easy to install, configure and maintain. SECURED BioNet does not use any of the standard operating systems, making it virtually hacker-proof! SECURED BioNet is the only device in market providing this level of security for enterprise WiFi LANs.