September 2008

Wireless Security – White Paper

Introduction

Over the years dependencies on WLAN technology has increased many fold. Number of hotspots and backhaul links on WiFi has seen sharp rise ever since de-licensing of 2.4 GHz and 5.8 GHz in most countries. With bandwidth cost coming down and laptop/PDA sales increasing we will see more WiFi deployments. Security of the network and protecting the user from stray attacks are of paramount importance to Brovis.

Brovis Wireless Networks is highly committed to providing rich network access with highly reliable security options. One may choose any of the security options listed below depending upon the network structure and the user access mechanism they wish to implement. This white paper examines various security options and their significance.

1. Access Control List

Brovis' Access Control List (ACL) allows an administrator to perform security actions based on the client station MAC address. This can be used to allow or deny association with the Access Point for unique per station encryption key assignment. By default, while the checking of the ACL is enabled, the ACL itself is empty. Therefore, an ACL entry must exist before enabling an ACL. While an ACL is enabled, stations with valid share keys and stations with matching "allow" entries on the ACL are authenticated. Alternatively, configuring the ACL to "strict" mode requires an ACL entry that specifies the station's assigned unique key or else the station is denied association. In strict mode, stations with valid share keys that are not on the ACL are not authenticated. The stations must have unique keys defined and matching "allow" ACL entries specified to associate with the AP. All of Brovis' wireless systems are equipped with "MAC ID Blacklisting" feature which allows the network administrator to blacklist a particular user from the network.

2. Wired Equivalent Privacy

WEP (Wired Equivalent Privacy) is 802.11's encryption standard implemented in the MAC Layer that BroVis equipment support. If a user activates WEP, the NIC encrypts the payload (frame body and CRC) of each 802.11 frame before transmission using an RC4 stream cipher provided by RSA Security. The receiving station, such as a Base Station or AP or CPE or wireless-NIC, performs decryption upon arrival of the frame. As a result, 802.11 WEP only encrypts data between 802.11 stations. Once the frame enters the wired side of the network, such as between access points, WEP no longer applies. WEP specifies a shared secret 40 or 64-bit key to encrypt and decrypt the data. We also include 128 bit keys (known as "WEP2"). With WEP, the receiving station must use the same key for decryption. Each wireless-NIC and AP, therefore, must be manually configured with the same key.

3. WPA Preshared Key

WPA preshared key (WPA-PSK) is best suited for small businesses and home wireless networks. A shared key, or password, is configured in the wireless access point and other wireless laptop or desktop devices. WPA-PSK generates a unique key for each session between a wireless client and the associated AP. The unique key used in the client-to-access-point communications makes reverse engineering of the preshared key more difficult for would -be attackers. WPA-PSK uses more advanced security techniques to encrypt and monitor the message stream. While WPA-PSK still uses the RC4 encryption standard used in WEP, it implements temporal key integrity protocol (TKIP), which provides per-packet key mixing, a message integrity check and a re-keying

mechanism. TKIP's algorithms and method-integrity checking techniques prevent the unwanted decryption of and tampering with packets in the wireless message stream. Brovis offers the latest WPA2 security standard for enhanced protection mechanism.

4. RADIUS Authentication

Brovis enables ease of authentication of the client devices by RADIUS Server through the Access Points. RADIUS is a common authentication protocol utilized by the IEEE 802.1X security standard. RADIUS improves the WEP encryption key standard, in conjunction with other security methods such as EAP-PEAP.

RADIUS is commonly used to facilitate secured roaming by companies which provide a single global set of credentials that are usable on many public networks. RADIUS facilitates this by the use of realms, which identify where the RADIUS server should forward the AAA requests for processing.

5. Temporal Key Integrity Protocol

Brovis introduced advanced security setup through the introduction of the TKIP security feature. The temporal key integrity protocol (TKIP), initially referred to as WEP2, is an interim solution that fixes the key reuse problem of WEP, that is, periodically using the same key to encrypt data. The TKIP process begins with a 128-bit "temporal key" shared among clients and access points. TKIP combines the temporal key with the client's MAC address and then adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. This procedure ensures that each station uses different key streams to encrypt the data. TKIP uses RC4 to perform the encryption, which is the same as WEP. A major difference from WEP, however, is that TKIP changes temporal keys every 10,000 packets. Through this Brovis Wireless Distribution system provides a dynamic distribution mechanism that significantly enhances the security of the network.

Brovis envisioned the use of TKIP as advantageous as the current wireless infrastructure deployed based on WEP-based access points and radio NICs can be upgraded to TKIP through relatively simple firmware patches. In addition, WEP-only equipment will still interoperate with TKIP-enabled devices using WEP.

6. Advanced Encryption Standards

Brovis recommends its users the use of Advanced Encryption Standard (AES). AES is the latest encryption standard used to protect data. The AES implements symmetric key cryptography as a block cipher and (at a minimum) support block sizes of 128-bit and key sizes of 128-bit, 192-bit, and 256-bit. It is a 128-bit (16 byte) block cipher with variable key sizes ranging from 128 bits to 256 bits. Through AES Brovis offers much higher security strength as compared to the DES standard that supports only 56-bit keys. Government, e-businesses and enterprises can use AES to strengthen the privacy and security of a wide variety of online transactions, ranging from cash-machine withdrawals to Internet shopping and sensitive e-mail applications..

7. WPA Preshared Key

WPA preshared key (WPA-PSK) is best suited for small businesses and home wireless networks. A shared key, or password, is configured in the wireless access point and other wireless laptop or desktop devices. WPA-PSK generates a unique key for each session between a wireless client

and the associated AP. The unique key used in the client-to-access-point communications makes reverse engineering of the preshared key more difficult for would-be attackers.

WPA-PSK uses more advanced security techniques to encrypt and monitor the message stream. While WPA-PSK still uses the RC4 encryption standard used in WEP, it implements temporal key integrity protocol (TKIP), which provides per-packet key mixing, a message integrity check and a re-keying mechanism. TKIP's algorithms and method-integrity checking techniques prevent the unwanted decryption of and tampering with packets in the wireless message stream.

8. Peer-Peer Isolation

Brovis implements P2P isolation for enhanced security. Brovis provides both Intra-VAP and Inter VAP isolation. Intra-VAP isolation disables laptops/desktops/PDA etc that's connected to an AP through a SSID. It isolates client devices connected on the same SSIDs. On the other hand Inter-VAP isolates the access among the client devices connected to different SSIDs of a MSSID AP. This feature protects the user from possible data theft while in a hotspot having any shared folders unprotected.

9. Rogue AP detection

Any AP installed without the permission of the network administrator is termed as a Rogue AP. This could be an AP that was brought into the organization and setup without permission by internal employees to allow them the flexibility wireless offers (while creating a back-door into the organization). On the other hand, a rogue AP could also be an AP installed on the internal network by a hacker or indeed penetration tester to allow them to access internal network resources while by bypassing network security devices (e.g. firewalls). All Brovis wireless systems have built –in Rogue AP that detects any stray AP and can isolate the same.

WiFi related Risk Issues

Although attacks against wireless networks will undoubtedly increase in number and sophistication over time, most of the current risks fall into seven basic categories:

- Insertion attacks
- Interception and unauthorized monitoring of wireless traffic
- Jamming
- Client-to-Client attacks
- Brute force attacks
- Encryption attacks

- Mis-configuration

Understanding how they work and using this information to prevent their entry is the way forward for any wireless solution.

1. Insertion Attacks

Insertion attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review. They can be:

- Unauthorized Clients
- Unauthorized or Renegade Access Points

2. Interception and Monitoring of Wireless Traffic

As in wired networks, it is possible to intercept and monitor network traffic across a wireless LAN. The attacker needs to be within range of an access point for this attack to work. All a wireless intruder needs is access to the network data stream. The interception & monitoring can happen through either of the following:

- Wireless Packet Analysis
- Broadcast Monitoring
- Access Point Clone Traffic Interception

3. Jamming

Denial of service attacks are also easily applied to wireless networks, where legitimate traffic can not reach clients or the access point because illegitimate traffic overwhelms the frequencies. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency, corrupting the signal until the wireless network ceases to function. In addition, devices that operate on the 2.4 GHz band can disrupt a wireless network using this frequency. These denials of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other wireless devices installed in other work areas that degrade the overall signal.

4. Client-to-Client Attacks

Two wireless clients can talk directly to each other, bypassing the access point. Users therefore need to defend clients not just against an external threat but also against each other. The predominant attacks include the following,

- File Sharing and Other TCP/IP Service Attacks
- DOS (Denial of Service)

5. **Brute Force Attacks (against Access Point Passwords)**

Most access points use a single key or password that is shared with all connecting wireless clients. Brute force dictionary attacks attempt to compromise this key by methodically testing every possible password. The intruder gains access to the access point once the password is guessed.

In addition, passwords can be compromised through less aggressive means. A compromised client can expose the access point. Not changing the keys on a frequent basis or when employees leave the organization also opens the access point to attack. Managing a large number of access points and clients only complicates this issue, encourages negligence in security practices.

6. **Attacks against Encryption**

The average hacker uses programs that do not attack the cryptosystem protocols themselves, but rather system specific implementations of encryption protocols. As it turns out, there are several "doable" attacks that can be launched by the typical hacker.
Passive attacks basically boil down to snooping or otherwise registering the user's activities while he is using encryption protocol. There are many passive attacks like, Key press snooping, Memory space snooping, Disk cache snooping, Packet sniffing

Active attacks go further. The attacker needs to actively interfere with the user's activities. Active attacks include Trojan horses and Reworked code

7. **Mis-configuration**

Many access points ship in an unsecured configuration in order to emphasize ease of use and rapid deployment. Unless administrators understand wireless security risks and properly configure each unit prior to deployment, these access points will remain at a high risk for attack or misuse.

Wireless Information Security Management

Process and technology are always easily confused, and ever more so than with wireless information security management. In fact, the same business processes that establish strong risk management practices for physical assets and wired networks also work to protect wireless resources. The following cost-effective guidelines help organizations to establish proper security protections as part of an overall wireless strategy. The following items are an introduction to this approach.

1. **Wireless Security Policy and Architecture Design** – Security policy, procedures and best practices should include wireless networking as part of overall security management architecture to determine what should be allowed with wireless technology.

2. **Access Point Configuration Policy** – Administrators need to define standard security settings for any access point before it can be deployed. These guidelines should cover SSID, WEP keys and encryption, and SNMP community words. Brovis recommends all system administrators to retain the installation report that Brovis engineers will handover during the sign-off phase.

3. **Managed Security Services for Wireless** – Brovis recommends MSS for any organization. MSS helps organizations establish effective security practices without the overhead of an extensive, in-house solution. MSS providers handle assessment, design, deployment, management and support across a broad range of information security disciplines. This 24/7/365 solution works with the customer to set policy and architecture, plus provides emergency response, if needed.

Conclusion

Brovis' commitment to delivering last mile access with rich security feature ensures that the network and the users connected to the network are fully secured. Brovis engages in a regular manner in enhancing programs and as an outcome end users will be assured of feature rich cutting edge technology.

For more information, please contact:

Brovis Wireless Networks Pvt Ltd

185/137, II Floor, SPS Building

Anna Salai, Chennai 600 002.

Ph: +91 44 42630014/15

Email: marketing@brovis.com