



## **COMMON WIRELESS SECURITY QUESTIONS AND ANSWERS**

### **QUESTIONS ABOUT STANDARDS: WEP WPA AND WPA2**

#### **WHAT IS WEP?**

Wired Equivalent Privacy is a security protocol defined by the IEEE Wireless Fidelity (WiFi) 802.11b standard designed to provide a similar level of security and privacy for a WLAN (wireless local area network) as commonly expected from a wired LAN (local area network). Wired LANs however, are physically protected because they are inside secure buildings unlike wireless networks that send data over radio waves not confined by physical barriers like walls and floors. WEP encrypts data sent over radio waves so that it is protected as it is transmitted from one end point to another.

#### **HOW SECURE IS WEP?**

WEP has been found to have a number of weaknesses. At its base, the encryption algorithm is flawed, making it susceptible to cracking. Also, the keys used for protection are unreliable and easily deciphered.

#### **SHOULD I USE WEP?**

It is better than no security at all, but it is not recommended.

#### **WHAT IS WPA?**

Wi-Fi Protected Access (WPA) is a data encryption specification for 802.11 wireless networks that replaces the weaker WEP. Created by WiFi Alliance before the 802.11i security standard was ratified by the IEEE, it improves on WEP by using dynamic keys, Extensible Authentication Protocol to secure network access, and an encryption method called Temporal Key Integrity Protocol (TKIP) to secure data transmissions.

#### **WHAT IS WPA2?**

Wi-Fi Protected Access 2 is an enhanced version of WPA. It is the official 802.11i standard that was ratified by the IEEE in June 2004. WPA2 is stronger than WPA because it uses Advanced Encryption Standard (AES) instead of RC-4/TKIP (see above). AES supports 128-bit, 192-bit and 256-bit keys. WPA2 can also use pre-shared keys or 802.1x authentication.

#### **WHAT ARE 802.11I AND 802.1X?**

These are new security standards developed by 802.11 that use advanced encryption technologies such as Advanced Encryption Standard (AES) and Temporal Key Integrity Protocol (TKIP), as well as secure key-distribution methods. 802.1x enables automatic changing of encryption keys at certain time intervals, for example every 5 minutes or so. By the time a hacker has intercepted a key and managed to decipher it, a new key has already replaced it.

## QUESTIONS ABOUT SETTINGS AND SOLUTIONS

### WHAT IS ENCRYPTION AND WHY IS IT IMPORTANT?

Encryption is a security measure that uses special technologies to scramble transmissions from one end to the other. One of the most popular forms of encryption uses special keys or codes enabling two computers to communicate: the sending computer transmits a key or code to the receiving computer and if the keys match, the sender is allowed into the system. Encryption is important because it prevents others from reading your messages, files and information.

### WHAT IS AN SSID?

Every wireless network, whether home or business, has a name consisting of up to 32 letters or numbers by which it can be identified – this is its Service Set Identifier (SSID). A wireless access point (AP) or router in open network mode will periodically broadcast a beacon signal along with the signal strength and functional capabilities of the AP, and the SSID to all wireless devices within range announcing that the network is live.

### I HAVE HEARD THAT DISABLING THE SSID BEACONING FUNCTIONALITY CAN STOP WARDRIVERS FROM ACCESSING MY WLAN. IS THIS TRUE?

This helps make your wireless network less susceptible, but it's still not failsafe. When you disable the beacon functionality, you need to know the SSID to access the connection. If you are not broadcasting, the hacker does not easily know the SSID to your network, but he can still intercept data packets as they travel between your access point and wireless client, vice versa. This data may reveal the SSID of your network.

### WHAT IS MAC FILTERING AND HOW EFFECTIVE IS IT?

Every Wi-Fi device has its own unique media access control (MAC) number. Networks can be configured to accept only certain MAC addresses and filter out the rest. MAC filtering is effective for small networks, but for larger networks it is not as useful as experienced hackers can imitate a MAC address by intercepting it and then programming their own computer to broadcast using this stolen MAC address.

### WHAT SECURITY SHOULD I USE? WEP; WPA OR WPA2?

You should use WPA2 as it is the most secure of all three options and uses AES encryption to protect data. After WPA2, WPA is the second most secure using Temporal Key Integrity Protocol (TKIP) to secure transmission. WEP is the least secure due to its flawed encryption algorithm.

### WHAT IS RADIUS?

Already in place in many corporations, remote access dial-up service (RADIUS), is another standard that protects access to wireless networks. RADIUS employs a user name and password scheme to allow only approved users access to the network – it does not affect or encrypt data. When a user wants access to network files, email programs or the internet, they submit their user name and password to the server, the server verifies that the user has an account, then verifies that the user is using the correct password, before granting access.

## WHAT IS KERBEROS?

Kerberos is a network authentication system based on key distribution, developed by MIT. Devices communicating over a wired or wireless network identify themselves to each other while preventing eavesdropping or replay attacks. After a client and server have identified themselves to one another, Kerberos enables their communication to be encrypted to assure privacy and data integrity, using cryptography systems such as data encryption standard (DES).

## LINKS TO HELPFUL RESOURCES

Wi-Fi alliance

<http://www.wi-fi.org>

Toshiba wireless products

[http://eu.computers.toshiba-europe.com/cgi-bin/ToshibaCSG/generic\\_content.jsp?service=EU&ID=ONLINE\\_SHOP](http://eu.computers.toshiba-europe.com/cgi-bin/ToshibaCSG/generic_content.jsp?service=EU&ID=ONLINE_SHOP)