Microsoft Knowledge Base Article - 815485

Overview of the WPA Wireless Security Update in Windows XP

View products that this article applies to.

IN THIS TASK

SUMMARY

This article discusses the new Wi-Fi Protected Access (WPA) update in Microsoft Windows XP.

The Institute of Electrical & Electronics Engineers (IEEE) 802.11i wireless networking standard specifies improvements to wireless local area networking (LAN) security. The 802.11i standard is currently in draft form, with ratification due at the end of 2003. The 802.11i standard addresses many of the security issues of the original 802.11 standard. While the new IEEE 802.11i standard is being ratified, wireless vendors have agreed on an interoperable interim standard known as Wi-Fi Protected Access (WPA).

back to the top

Features of WPA Security

The following security features are included in the WPA standard:

WPA Authentication

802.1x authentication is required in WPA. In the 802.11 standard, 802.1x authentication was optional.

For environments without a Remote Authentication Dial-In User Service (RADIUS) infrastructure, WPA supports the use of a preshared key. For environments with a RADIUS infrastructure, Extensible Authentication Protocol (EAP) and RADIUS is supported.

back to the top

WPA Key Management

With 802.1x, the rekeying of unicast encryption keys is optional. Additionally, 802.11 and 802.1x provide no mechanism to change the global encryption key used for multicast and broadcast traffic. With WPA, rekeying of both unicast and global encryption keys is required. For the unicast encryption key, the Temporal Key Integrity Protocol (TKIP) changes the key for every frame, and the change is synchronized between the wireless client and the wireless access point (AP). For the global encryption key, WPA includes a facility for the wireless AP to advertise the changed key to the connected wireless clients.

back to the top

Temporal Key Integrity Protocol (TKIP)

For 802.11, Wired Equivalent Privacy (WEP) encryption is optional. For WPA, encryption using TKIP is required. TKIP replaces WEP with a new encryption algorithm that is stronger than the WEP algorithm but that uses the calculation facilities present on existing wireless devices to perform encryption operations. TKIP also provides for the following:

- The verification of the security configuration after the encryption keys are determined.
- The synchronized changing of the unicast encryption key for each frame.
- The determination of a unique starting unicast encryption key for each preshared key authentication.

back to the top

Michael

With 802.11 and WEP, data integrity is provided by a 32-bit *integrity check value* (ICV) that is appended to the 802.11 payload and encrypted with WEP. Although the ICV is encrypted, you can use cryptanalysis to change bits in the encrypted payload and update the encrypted ICV without being detected by the receiver.

With WPA, a method known as *Michael* specifies a new algorithm that calculates an 8-byte *message integrity code* (MIC) using the calculation facilities available on existing wireless devices. The MIC is placed between the data portion of the IEEE 802.11 frame and the 4-byte ICV. The MIC field is encrypted together with the frame data and the ICV.

Michael also provides replay protection. A new frame counter in the IEEE 802.11 frame is used to prevent replay attacks.

back to the top

AES Support

WPA defines the use of Advanced Encryption Standard (AES) as an additional replacement for WEP encryption. Because you may not be able to add AES support through a firmware update to existing wireless equipment, support for AES is optional and is dependant on vendor driver support.

back to the top

Supporting a Mixture of WPA and WEP Wireless Clients

To support the gradual transition of WEP-based wireless networks to WPA, a wireless AP can support both WEP and WPA clients at the same time. During the association, the wireless AP determines which clients use WEP and which clients use WPA. The disadvantage to supporting a mixture of WEP and WPA clients is that the global encryption key is not dynamic. This is because WEP-based clients cannot support it. All other benefits to the WPA clients, such as integrity, are maintained.

back to the top

Changes Required to Support WPA

WPA requires software changes to the following:

- Wireless access points
- Wireless network adapters
- Wireless client programs

back to the top

Changes to Wireless Access Points

Wireless access points must have their firmware updated to support the following:

- **The new WPA information element**
  To advertise their support of WPA, wireless APs send the beacon frame with a new 802.11 WPA information element that contains the wireless AP's security configuration (encryption algorithms and wireless security configuration

information).
- **The WPA two-phase authentication**
  Open system, then 802.1x (EAP with RADIUS or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless access points to support WPA, obtain a WPA firmware update from your wireless AP vendor and upload it to your wireless AP.

back to the top

Changes to Wireless Network Adapters

Wireless network adapters must have their firmware updated to support the following:

- **The new WPA information element**
  Wireless clients must be able to process the WPA information element and respond with a specific security configuration.
- **The WPA two-phase authentication**
- Open system, then 802.1x (EAP or preshared key).
- **TKIP**
- **Michael**
- **AES** (optional)

To upgrade your wireless network adapters to support WPA, obtain a WPA update from your wireless network adapter vendor and update the wireless network adapter driver.

For Windows wireless clients, you must obtain an updated network adapter driver that supports WPA. For wireless network adapter drivers that are compatible with Windows XP (Service Pack 1) and Windows Server 2003, the updated network adapter driver must be able to pass the adapter's WPA capabilities and security configuration to the Wireless Zero Configuration service.

Microsoft has worked with many wireless vendors to embed the WPA firmware update in the wireless adapter driver. So, to update you Windows wireless client, all you have to do is obtain the new WPA-compatible driver and install the driver. The firmware is automatically updated when the wireless network adapter driver is loaded in Windows.

back to the top

Changes to Wireless Client Programs

Wireless client programs must be updated to permit the configuration of WPA authentication (and preshared key) and the new WPA encryption algorithms (TKIP and the optional AES component).

For wireless clients that are running Windows XP service pack 1 (SP1) and later or Windows Server 2003 and that are using a wireless network adapter that supports the Wireless Zero Configuration service, you must obtain and install the Windows WPA Client. The Windows WPA Client updates the wireless network configuration dialog boxes to support new WPA options.

To obtain the WPA client program, visit the following Microsoft Web site:

 Download the Windows XP i386 package

For wireless clients running Windows 2000 (or clients running Windows XP SP1 or Windows Server 2003 and using a wireless network adapter that does not support the Wireless Zero Configuration service), you must obtain and install a new WPA-compliant configuration tool from your wireless network adapter vendor.

back to the top

Related Intel Information

For information about an Intel issue with this update, visit the following Intel Web site:

http://www.intel.com/support/network/wireless/pro2100/sb/cs-006131-prd944.htm

The third-party products that are discussed in this article are manufactured by companies that are independent of Microsoft. Microsoft makes no warranty, implied or otherwise, regarding the performance or reliability of these products. Microsoft provides third-party contact information to help you find technical support. This contact information may change without notice. Microsoft does not guarantee the accuracy of this third-party contact information.

The information in this article applies to:

- Microsoft Windows XP Home Edition
- Microsoft Windows XP Professional

Last Reviewed: 10/28/2003 (1.3)

Keywords: kbenv kbnetwork kbDriver kbinfo KB815485