ARTICLE

Axis Network Print Servers

Wireless Security Terminology Explained

Created: April 21, 2005
Last updated: April 21, 2005
Rev: 1.0

TABLE OF CONTENTS

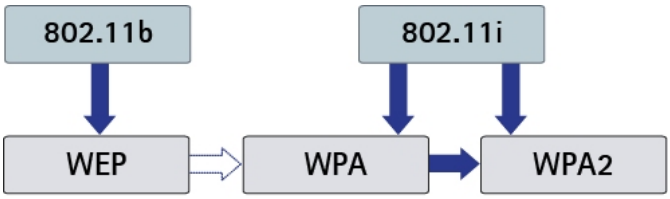
Introduction

How have the wireless security standards evolved over the past few years and how do they work on a high-level? This article explains the terminology and lays the ground for undestanding wireless security concepts.

1 Wireless Security

Wireless print servers are a convenient way to get access to printers without any cables. Wireless printing can provide the same level of privacy and security as wired printing, provided that the wireless devices are configured to use appropriate security. The type of security you choose will depend on the wireless standards supported by the access point or wireless card you are using and the level of security required.
Basically, there are three security standards to consider:

- WEP (Wired Equivalent Privacy)
- WPA (WiFi Protected Access)
- WPA2



Relationship between WEP, WPA and WPA2

WEP was designed together with 802.11b some years back, and exists in all wireless equipment. Unfortunately, it has several inherent weaknesses, one of them being that the encryption key is frequently reused, making it possible to break the encryption in a matter of minutes on a wireless network with a lot of traffic. IEEE (Institute of Electrical and Electronics Engineers) recognized these problems, and another workgroup, 802.11i, was formed to address these.

The Wi-Fi Alliance is a nonprofit international association formed in 1999 to certify interoperability of wireless local area network products based on the IEEE 802.11 specification. The Wi-Fi Alliance couldn't wait the several years it takes to agree upon a standard, so they created their own standard called WPA (WiFi Protected Access), which is based on a preliminary draft from 802.11i. WPA has since been the industry standard.

As mentioned, encryption key reuse was the main problem of WEP. WPA overcame this design flaw by introducing TKIP (Temporal Key Integrity Protocol).

Recently, the IEEE802.11i workgroup finished their work, which resulted in changing the encryption method from TKIP to CCMP (Counter Mode-CBC MAC Protocol). The crypto algorithm RC4, used in both WEP and WPA, was exchanged for AES (Advanced Encryption Standard), making it possible for wireless devices to be FIPS 140-2 certified for US Federal government use.

Shortly thereafter, the WiFi Alliance released its updated WPA2 standard to cover all aspects of the 802.11i standard.

Using WPA or WPA2 authentication and a random password with 20 characters is considered secure, while WEP is not. To ensure backwards compatibility, AXIS OfficeBasic USB Wireless G Print Server supports all three industry encryption standards.

2 Authentication

Both WPA and WPA2 come in two versions, enterprise and personal. In the enterprise version, users are authenticated with a RADIUS server (Remote Authentication Dial-In User Service), using the 802.1X authentication framework.

The personal version does not require user authentication with a RADIUS server. Devices are authenticated using a pre-shared key (PSK), which is used to configure all network units. This version is also called WPA-PSK (or WPA2-PSK). As with any password, the pre-shared key must be chosen wisely (e.g. through the use of a combination of letters and numbers) so it cannot be cracked.

Both versions offer similar levels of security; however the enterprise version scales better in larger organizations, where it is impractical to set the PSK in each network unit.

AXIS OfficeBasic USB Wireless G supports both WPA-PSK and WPA2-PSK.

REFERENCES:
WiFi Alliance: www.wi-fi.org
IEEE: http://standards.ieee.org