

Seguridad en redes Wi-Fi

Jesús Rodríguez Heras
Juan Pedro Rodríguez Gracia

Alumnos colaboradores de: **Mercedes Rodríguez García**

Índice general

1. WPA2	5
1.1. ¿Qué es WPA2?	5
1.1.1. WPA2-Personal	5
1.1.2. WPA2-Enterprise	5
2. Espionaje en red WPA2-PSK	7
2.1. Conocemos la passphrase	7
2.2. No conocemos la passphrase	7

Capítulo 1

WPA2

1.1. ¿Qué es WPA2?

Es un protocolo de seguridad, desarrollado por la Wi-Fi Alliance, que cifra los mensajes en las redes inalámbricas para permitir comunicaciones seguras entre un host y un punto de acceso.

WPA2 salió al mercado en 2004 con el estándar 802.11i (o IEEE 802.11i-2004) e incluye soporte para CCMP¹.

Tenemos dos versiones de WPA2:

1.1.1. WPA2-Personal

Es conocido también como “WPA2-PSK”. Está diseñado para redes domésticas y pequeñas oficinas y no requiere un servidor de autenticación. Cada dispositivo de la red inalámbrica encripta el tráfico de red derivando su clave de cifrado de una clave compartida. Esta clave se puede ingresar como una cadena o como una **passphrase** de caracteres ASCII.

1.1.2. WPA2-Enterprise

También se conoce como “WPA2 802.11i mode”. Está diseñado para redes empresariales y requiere de un servidor RADIUS de autenticación. Lo que requiere una mayor configuración pero proporciona mayor seguridad.

¹CCMP es un modo de encriptación basado en AES con gran seguridad.

Capítulo 2

Espionaje en red WPA2-PSK

De las dos versiones de WPA2 existentes, nos centraremos en WPA2-PSK para la práctica.

2.1. Conocemos la passphrase

2.2. No conocemos la passphrase