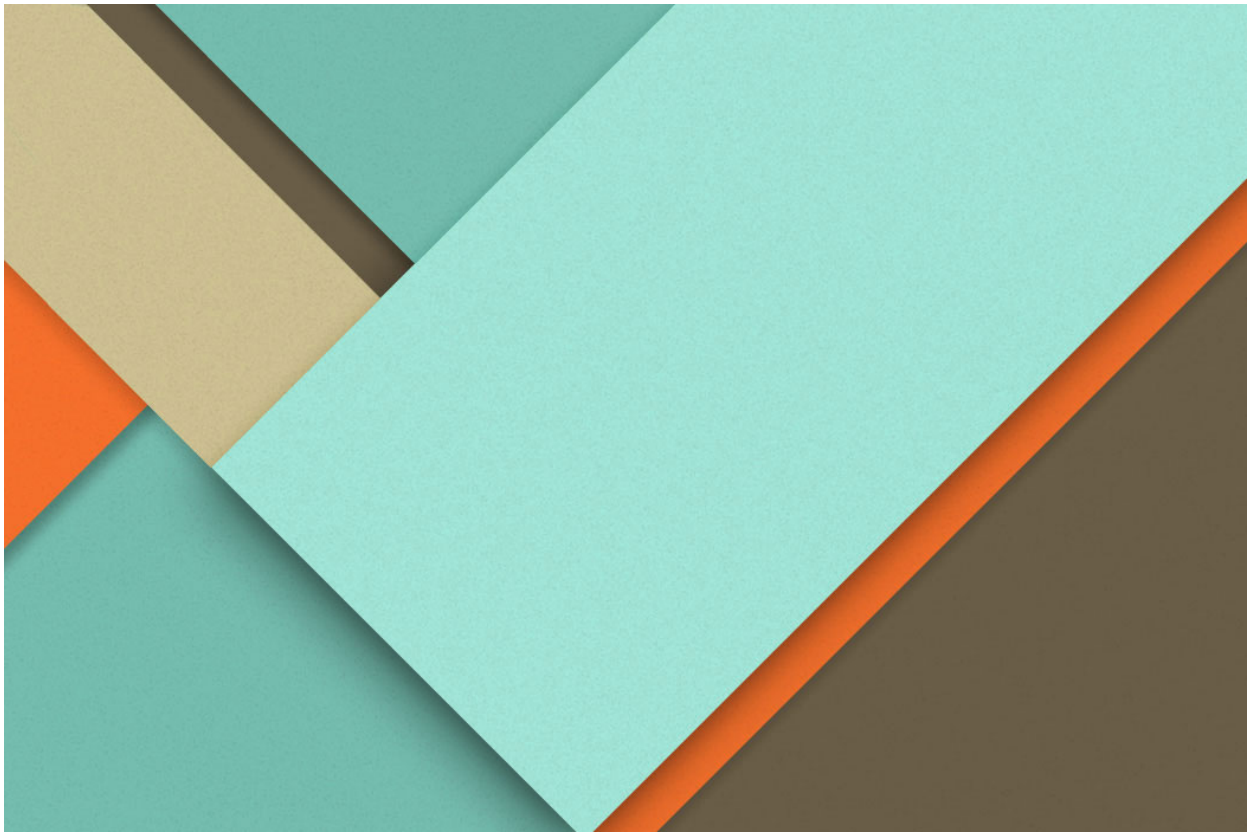


SEGURIDAD EN WI-FI

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

Beneficios del Wi-Fi

La conexión a redes WiFi nos ha proporcionado unas prestaciones extraordinarias a la hora de disfrutar de todo tipo de contenidos en internet. Por fin podíamos decir adios a los cables... o casi. Y sin embargo, esa comodidad ha estado siempre comprometida por la seguridad de esas conexiones, que una y otra vez ha demostrado ser insuficiente.

Las vulnerabilidades en los distintos protocolos de seguridad inalámbricos han ido apareciendo de forma sistemática, y a la desastrosa seguridad del protocolo WEP se han sumado las vulnerabilidades que también afectaron al protocolo WPA y, por último, al protocolo WPA2 que parecía protegernos de forma razonable. Así es como nuestras redes WiFi han ido cayendo unas detrás de otras.

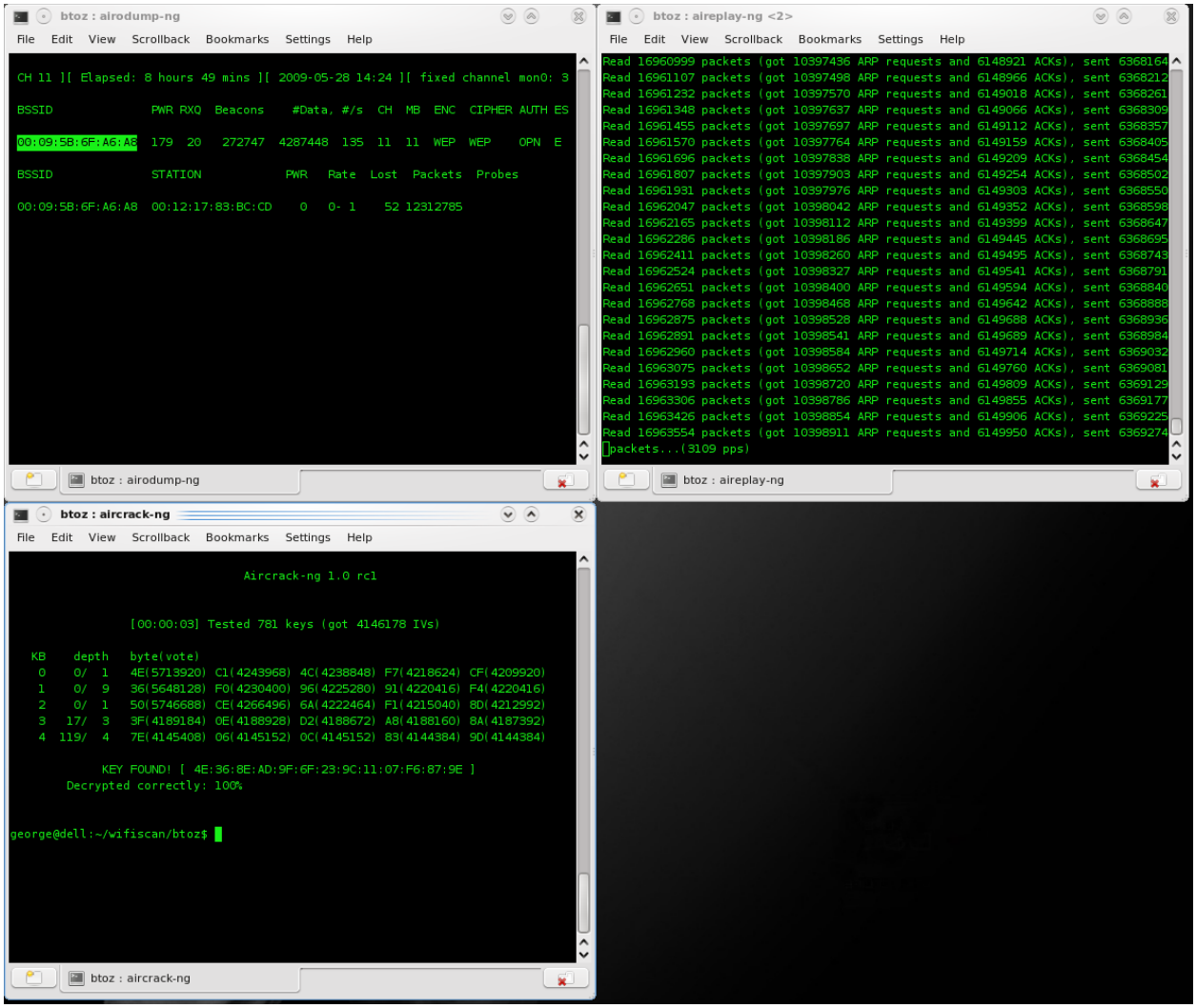
WEP, casi un juego de niños para los hackers

El lanzamiento del estándar IEEE 802.11 para conexiones inalámbricas que se ratificó en 1997 incluyó un apartado para la seguridad de esas conexiones: el llamado Wired Equivalent Privacy (WEP) —curioso que el acrónimo haga uso de la palabra "Wired" y no "Wireless", por cierto— planteaba un algoritmo de seguridad para proteger la confidencialidad de los datos de forma similar a la que se proporcionaba a redes de cable.

El protocolo WEP hacía uso del cifrado RC4 y del mecanismo CRC-32 para la integridad, y el sistema estándar de 64 bits hacía uso de una clave de 40 bits que se concatenaba con un vector de inicialización (IV) de 24 bits para conformar la clave RC4. A cualquiera que haya usado este protocolo le resultarán familiares esas clave WEP de 64 bits, pero en formato hexadecimal, que hacían que al conectarnos a una red WiFi con esa seguridad tuviésemos que introducir esos diez caracteres exadecimales (números del 0 al 9, letras de la A a la F).

Aquel protocolo demostró su debilidad en 2001, cuando Scott R. Fluhrer, Itsik Mantin y Adi Shamir publicaron un estudio sobre los problemas del cifrado RC4 y cómo descifrar esas claves era posible en un tiempo reducido espiando una de estas conexiones e inspeccionando los paquetes que se iban intercambiando un cliente conectado a un punto de acceso. De hecho si el

tráfico era bajo, era posible inyectar y "estimular" paquetes de respuesta que servían para lograr que la cantidad de IVs permitiese luego encontrar la clave de acceso WiFi.



Specifications

Aquel tipo de ataque se volvió uno de los clásicos de los aficionados al hacking WiFi, y suites de seguridad como la archiconocida aircrack-ngpermitieron crackear una conexión WiFi con el protocolo WEP en apenas unos minutos.

A pesar de que la vulnerabilidad se conocía ampliamente, las operadoras mantuvieron su validez durante años, predefiniendo redes WiFi en los routers que suministraban a los clientes en las que se usaba el protocolo WEP por defecto.

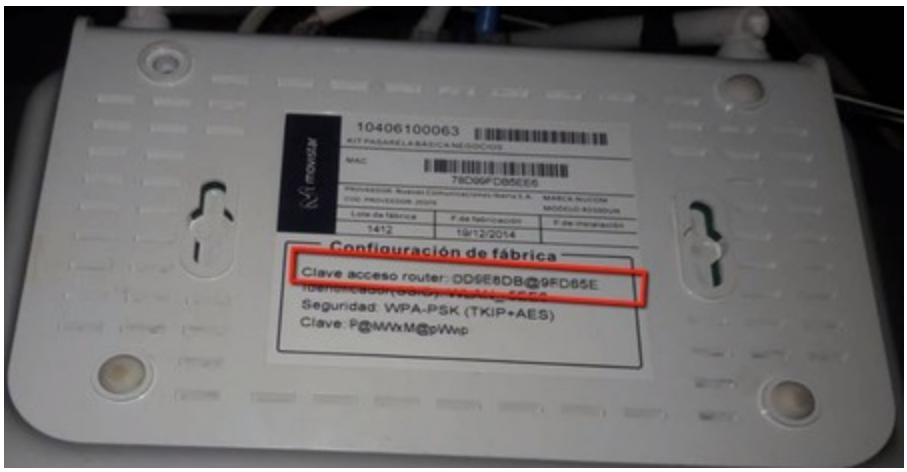
El propio FBI acabó mostrando lo fácil que era romper la seguridad esas redes en 2005, pero el verdadero detonante del caos WEP fue la brecha de seguridad en TJ Maxx, uno de los gigantes comerciales de Estados Unidos. Allí un hacker llamado Albert Gonzalez —capturado y condenado

a 20 años de cárcel— lograron robar más de 100 millones de cuentas de usuario, lo que le supuso unas pérdidas estimadas que rondaron los 1.000 millones de dólares.

Aquello fue la gota que colmó el vaso, y la industria y los usuarios por fin tomaron conciencia del peligro y se comenzó a dejar de usar el protocolo WEP por parte de fabricantes de equipos de comunicaciones y operadoras. Aquellas vulnerabilidades se trataron de parchear con claves más largas de hasta 256 bits o variaciones como WEP2 o WEPplus, pero el protocolo que trataría de atajar los problemas —sin lograrlo— ya estaba funcionando desde hacía años. WPA parecía la solución a nuestros problemas, pero claro, no lo era.

WPA como solución de transición

Aquellos enormes fallos al concebir un protocolo de seguridad para las comunicaciones inalámbricas trataron de corregirse con el desarrollo del estándar IEEE 802.11i, que no llegaría hasta un año después. La urgencia de la situación hizo que la Wi-Fi Alliance sacara una versión preliminar de ese estándar, y es así como en 2003 apareció en escena el protocolo Wi-Fi Protected Access (WPA).



Una de las ideas de WPA era poder ser aplicable como una actualización del firmware de muchos routers y otros equipos de comunicaciones, pero resultó que los puntos de acceso y routers necesitaban contar con algunos requisitos adicionales, lo que hizo que muchos routers "antiguos" no pudieran ser actualizados.

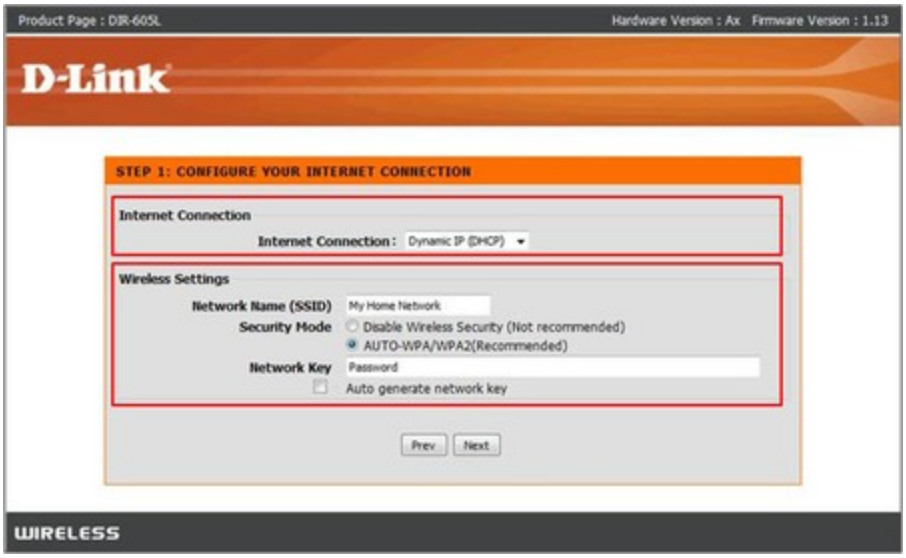
El protagonista de ese protocolo WPA que cumplía con parte de la especificación IEEE 802.11i era el llamado Temporal Key Integrity Protocolo (TKIP), que se diferenciaba del protocolo WEP en un tema clave: mientras que la clave tradicional WEP de 64 o 128 bits no cambiaba, con TKIP se implementaba una "clave por paquete", lo que hacía que se generara una nueva clave de 128 bits por cada paquete, algo que evitaba que este protocolo fuera vulnerable a los ataques que afectaban al protocolo WEP.

En este protocolo se usaba además un Message Integrity Check (MIC) de 64 bits —conocido popularmente como MICHAEL—, que servía para proporcionar integridad a todo el sistema, pero de nuevo se comprobó que aquello no era suficiente para asegurar estas conexiones. Martin Beck —uno de los creadores de la suite aircrack-ng— y Erik Twes —de la Universidad Técnica de Darmstadt— desmotraron en 2008 cómo los ataques a las redes WPA eran factibles haciendo uso de parte de lo que ya se había logrado en los célebres ataques Chopchop a las redes WEP. Su documento 'Practical attacks against WEP and WPA" (PDF) se convirtió en todo un referente en este tipo de estudios, pero este documento solo fue el principio.

Pronto aparecerían variaciones como la de Mathy Banhoef y Frank Piessens, que con su 'Practical Verification of WPA-TKIP Vulnerabilities" (PDF) fueron aún más allá y lograron demostrar cómo era posible inyectar paquetes y descifrarlos, algo que podía ser aprovechado para "secuestrar una sesión TCP" e inyectar código malicioso.

Las contraseñas WiFi, talón de aquiles de WPA (y WPA2)

A este protocolo le fallaba otra pata: la de las contraseñas. Aunque los fabricantes de equipos de comunicaciones (routers, puntos de acceso) establecían contraseñas relativamente fuertes por defecto para proteger las redes WiFi predefinidas en sus equipos, los usuarios acababan renombrando sus redes y cambiándoles las contraseñas por otras fáciles de recordar.



No es mala idea cambiar la contraseña por defecto de tu router, pero si lo haces, elige una contraseña fuerte en la que combines una longitud aceptable y caracteres de todo tipo.

Esas contraseñas débiles acababan siendo el verdadero problema de unas redes WiFi que quedaban desprotegidas ante los ataques de fuerza bruta con diccionario. Las suites como

aircrack-ng y las distribuciones Linux dedicadas a la auditoría de seguridad se hicieron famosas por integrar herramientas capaces de atacar redes WiFi que usaran el protocolo WPA.

Estas suites permitían forzar a un cliente a desconectarse para volver a negociar la conexión con el punto de acceso, algo que daba acceso al llamado 4-way TKIP handshake, resultado de esa negociación y suficiente para tratar de descifrar la contraseña WiFi por fuerza bruta a través (normalmente) del uso de un diccionario.

Hoy en día se pueden realizar auditorías WiFi hasta con smartphones y tablets, y existen adaptadores WiFi USB especialmente aptos para este tipo de propósitos.

Estos diccionarios contienen habitualmente millones de palabras del lenguaje normal, pero también se pueden generar a partir de combinaciones de todo tipo de caracteres para formar palabras de cualquier longitud. Esos diccionarios permiten comparar el handshake con cada palabra del diccionario, y si está en ellos, el atacante logra obtener la contraseña.

El proceso es habitualmente largo y costoso en potencia de computación, y no siempre es efectivo: la clave está en el uso de contraseñas fuertes, y esos ataques de diccionario y fuerza bruta están destinados a descifrar contraseñas WiFi de redes WPA (y WPA2) que son débiles por longitud o por usar palabras muy populares. La capacidad de cálculo necesaria para acelerar los cálculos ha hecho que hayan aparecido herramientas que usan GPUs en lugar de CPUs para hacer esos cálculos (hashcat es una de las más conocidas), y existen servicios como GPUhash o OnlineHashCrack que te ayudan a descifrar esos handshakes de forma gratuita y sin que uses tus propios recursos.

WPS, buenas intenciones, implementación desastrosa

Uno de los problemas que imponían las conexiones WiFi era lo incómodo que era conectar cierto tipo de dispositivos para que aprovechasen esta capacidad. Las impresoras, por ejemplo, planteaban la necesidad de facilitar el sistema de conexión basado en introducir la contraseña WiFi en cada momento.

Así es como nació Wi-Fi Protected Setup (WPS), un estándar para crear una red inalámbrica doméstica segura que la Wi-Fi Alliance lanzó en el año 2006. La idea era estupenda, porque hacía que si el router y el cliente disponían de esta capacidad, que uno se conectase al otro fuera cuestión de pulsar un botón.

Sin embargo WPS acabó convirtiéndose en una condena más para la seguridad de las conexiones WPA y WPA2. Una vulnerabilidad detectada en diciembre de 2011 por parte de Stefan Viehböck dejaba claro que aquel protocolo estaba expuesto a un ataque que permitía conseguir la clave WiFi sin necesidad de diccionarios o del proceso con el que hasta entonces se podían atacar a las redes WPA y WPA2.

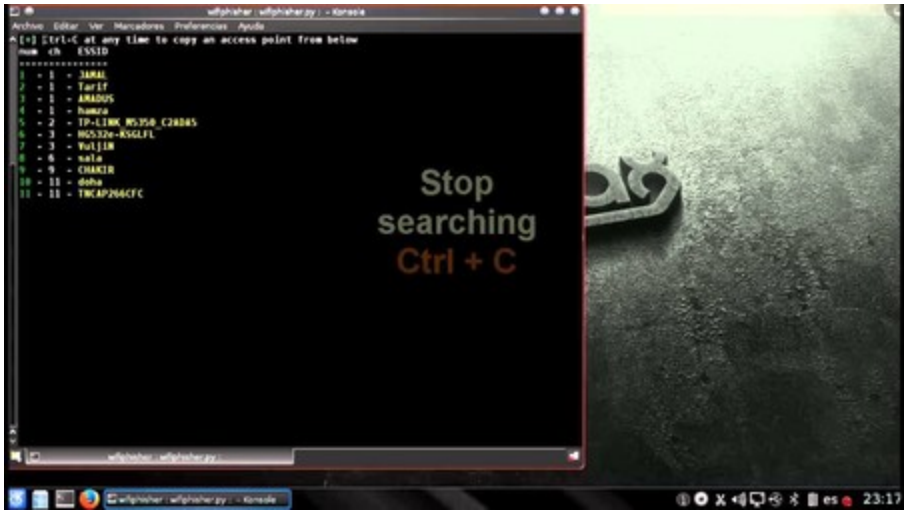
En su documento 'Brute forcing Wi-Fi Protected Setup" (PDF) este investigador demostraba cómo un ataque por fuerza bruta hacía factible superar la seguridad de los protocolos WPA y WPA2, y concluía con una recomendación a los usuarios: desactivar WPS, algo que de hecho no todos los routers facilitaban o incluso hacían posible.

Ese ataque online tuvo una alternativa offline con el ataque "Pixie Dust" descubierto en 2014 por Dominique Bongard, que no estaba siempre disponible pero que sí afectaba a unos cuantos fabricantes de chips WiFi. Tanto el uno como el otro fueron integrados en sucesivas versiones de

suites de seguridad y auditoría con herramientas como pixieWPS o Reaverque permitían atacar a este tipo de redes de forma automática y transparente para los usuarios.

WPA2: creíamos que estábamos a salvo, pero no era así

Hace la friolera de 13 años que tenemos teórico protocolo seguro para nuestras redes WiFi. Fue en 2004 cuando se lanzó por fin WPA2, la segunda versión de WPA que era de hecho la implementación del estándar IEEE 802.11i.



Las herramientas para realizar auditorías automatizadas a redes WiFi de todo tipo son cada vez más avanzadas y más sencillas de usar. Wifiphisher corriendo sobre Wifislax es un buen ejemplo de estas soluciones.

En WPA2 se sustituyen tanto TKIP como el cifrado RC4 que se usó tanto en WEP y en WPA con dos alternativas de cifrado y autenticación más fuertes. En primer lugar, el Advanced Encryption Standard (AES), y en segundo, el llamado Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). Era además posible configurar WPA2 con TKIP como forma de mantener la compatibilidad hacia atrás.

El protocolo ha demostrado ser mucho más resistente a ataques que sus predecesores, pero eso no significa que sea inmune. La vulnerabilidad llamada Hole196 aprovecha la implementación del Group Temporal Key (GTK), que teóricamente hacía uso de un sistema aleatorio que impedía ataques a esa parte del sistema. Sin embargo el uso de un generador de números aleatorios (RNG) específico utilizado por ciertos fabricantes hacía predecible ese GTK, lo que a su vez hacía vulnerable el protocolo.

A ese problema se le suman al menos otros dos. El primero, una vez más, el uso de contraseñas débiles que pueden también ser descifradas mediante ataques de fuerza bruta como los

anteriormente descritos. El segundo, el uso de métodos alternativos de ingeniería social que engañen al usuario.

Este es el tipo de páginas de reconexión falsas que pueden generar este tipo de herramientas para engañar al usuario y que "confiese" la contraseña WiFi de su red inalámbrica.

Es algo así como "si no puedes capturar la contraseña directamente, pídesela al usuario". Un atacante puede usar herramientas como Fluxionpara desconectar a un cliente (usuario) de su red WiFi y generar una página web que simule la que generaría su router. Esto haría creer al usuario que se ha perdido la conexión por algún conflicto y que con introducir la contraseña a su red WiFi desaparecerá el problema: lo que está haciendo en realidad es confesarle al atacante esa contraseña WiFi sin darse cuenta.

El anuncio de hoy del investigador de seguridad Mathy Vanhoef vuelve no obstante a demostrar que nuestras conexiones WiFi siguen sin estar protegidas aun cuando usemos el protocolo WPA2. Los llamados KRACKs (Key Reinstallation AttaCKs) permiten que los atacantes puedan "acceder a la información que hasta ahora se asumía que estaba cifrada de forma segura".

El ataque permite por tanto acceder a información sensible que transmitimos a través de nuestras conexiones WiFi, tal como números de tarjetas de crédito, contraseñas, mensajes de chat, correos o fotos, y "funciona con todas las redes WiFi", siendo además posible en algunas de ellas "inyectar y manipular los datos".

¿Hay solución? Sí: la de que los fabricantes ofrezcan una actualización del firmware de sus equipos de comunicaciones y los responsables de nuestros dispositivos móviles (portátiles, smartphones y tablets sobre todo) también ofrezcan esos parches para atajar el problema. Lamentablemente es probable que en muchos casos esas actualizaciones tarden en llegar o incluso no lleguen nunca, por lo que hacer uso de mecanismos adicionales (VPNs, conexiones seguras HTTPS) también ayudará a proteger nuestros datos sensibles.