

XI
JORNADAS
STIC
CCN-CERT

Ciberamenazas_
El reto de compartir

#XIJornadasCCNCERT

MADRID.
13 Y 14 DE DICIEMBRE
2017

KRACK ATTACKS



- Deepak Daswani
- Experto en Ciberseguridad, Conferenciante y Colaborador de Medios de Comunicación
- deepak@deepakdaswani.es

Índice

1. **Antecedentes y Contexto Actual de la Seguridad en Redes Wifi**
2. **Krack Attacks: Resumen ejecutivo**
3. **4-way Handhsake: Vulnerabilidad y Ataque**
4. **Demo**
5. **Conclusiones**

Lo que sabíamos hasta ahora



Internet
WiFi))
Gratuito

Lo que sabíamos hasta ahora

Cifrado WEP

- Presentado en 1999
- Utiliza cifrado RC4
- Claves de 64 bits o 128 bits
- Vector de inicialización de 24 bits
- Considerado como inseguro desde hace años por múltiples debilidades:
 - RCA de 40 bits
 - 16 millones de posibles IVs
 - CRC32 sólo sirve para solucionar errores involuntarios
- Herramientas de botón gordo que permitían romper una clave WEP en cuestión de minutos



Lo que sabíamos hasta ahora



Lo que sabíamos hasta ahora

Cifrado WPA

- Creado para corregir las deficiencias del WEP
- Autenticación mediante Radius o WPA-PSK
- RC4 de 128 bits e IVs de 48 bits
- TKIP cambia dinámicamente las claves a medida que es utilizado
- Se sustituye CRC por MIC (Message Integrity Code)
- Incluye protección contra ataques de repetición, ya que incluye un contador de tramas



Lo que sabíamos hasta ahora

Cifrado WPA2

- WPA es pre-estándar y WPA2 es el estándar
- AES en lugar de RC4
- CCMP en lugar de TKIP
- AES-CCMP + 4-way handshake son la fortaleza de WPA2
- La clave de cifrado es diferente para cada dispositivo
- WPA2-PSK es vulnerable a ataques de fuerza bruta o diccionario siempre que se capture el 4- way handshake (EAPOL)
- Vulnerabilidad en WPS descubierta por Stefan Viehböck en 2011



¿Qué ha pasado ahora?

KRACK attack: Wi-Fi connections vulnerable to hackers after flaw discovered

By Peter Marsh

Updated 24 Oct 2017, 3:52am

A security flaw has been discovered that could be used to hack into any device that uses Wi-Fi.

That includes your phone, your laptop, your PlayStation and your smart fridge.

The key reinstallation attacks, or **KRACKs**, were discovered by Belgian researcher Marty Vanhoef and are so serious the US Department of Homeland Security has issued an official warning.



Alarma por KRACK: todas las conexiones WiFi del mundo están en peligro

Un investigador belga reveló fallas de seguridad en los sistemas de los routers. Cualquiera de estas redes inalámbricas puede ser hackeada.

ABC TECNOLOGÍA

Buscar en ABC



Acceso / Registro

ESPAÑA INTERNACIONAL ECONOMÍA OPINIÓN DEPORTES CONOCER MOTOR FAMILIA GENTE SUMMUM CULTURA & OCIO SERVICIOS EDICIONES MADRID ABCSEVILLA

KRACK

Cómo protegerse del fallo de las redes WiFi tras romper el protocolo WPA2

- Los expertos en seguridad informática insisten en la necesidad de instalar los parches de seguridad que los fabricantes de tecnología manden en los próximos días, ya que un cambio en las claves del router WiFi no evita un posible ataque y robo de datos

Key Reinstallation Attacks

Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2

Mathy Vanhoef
imec-DistriNet, KU Leuven
Mathy.Vanhoef@cs.kuleuven.be

Frank Piessens
imec-DistriNet, KU Leuven
Frank.Piessens@cs.kuleuven.be

ABSTRACT

We introduce the key reinstallation attack. This attack abuses design or implementation flaws in cryptographic protocols to reinstall an already-in-use key. This resets the key's associated parameters such as transmit nonces and receive replay counters. Several types of cryptographic Wi-Fi handshakes are affected by the attack.

All protected Wi-Fi networks use the 4-way handshake to generate a fresh session key. So far, this 14-year-old handshake has remained free from attacks, and is even proven secure. However, we show that the 4-way handshake is vulnerable to a key reinstallation attack. Here, the adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying handshake messages. When reinstalling the key, associated parameters such as the incremental transmit packet number (nonce) and receive packet number (replay counter) are reset to their initial value. Our key reinstallation attack also breaks the PeerKey, group key, and Fast BSS Transition (FT) handshake. The impact depends on the handshake being attacked, and the data-confidentiality protocol in use. Simplified, against AES-CCMP an adversary can replay and decrypt (but not forge) packets. This makes it possible to hijack TCP streams and inject malicious data into them. Against WPA-TKIP and GCMP the impact is catastrophic: packets can be replayed, decrypted, and forged. Because GCMP uses the same authentication key in both communication directions, it is especially affected.

Finally, we confirmed our findings in practice, and found that every Wi-Fi device is vulnerable to some variant of our attacks. Notably, our attack is exceptionally devastating against Android 6.0: it forces the client into using a predictable all-zero encryption key.

KEYWORDS

work, we present design flaws in the 4-way handshake, and in related handshakes. Because we target these handshakes, both WPA- and WPA2-certified products are affected by our attacks.

The 4-way handshake provides mutual authentication and session key agreement. Together with (AES)-CCMP, a data-confidentiality and integrity protocol, it forms the foundation of the 802.11i amendment. Since its first introduction in 2003, under the name WPA, this core part of the 802.11i amendment has remained free from attacks. Indeed, the only currently known weaknesses of 802.11i are in (WPA-)TKIP [57, 66]. This data-confidentiality protocol was designed as a short-term solution to the broken WEP protocol. In other words, TKIP was never intended to be a long-term secure solution. Additionally, while several attacks against protected Wi-Fi networks were discovered over the years, these did not exploit flaws in 802.11i. Instead, attacks exploited flaws in Wi-Fi Protected Setup (WPS) [73], flawed drivers [13, 20], flawed random number generators [72], predictable pre-shared keys [45], insecure enterprise authentication [21], and so on. That no major weakness has been found in CCMP and the 4-way handshake, is not surprising. After all, both have been formally proven as secure [39, 42]. With this in mind, one might reasonably assume the design of the 4-way handshake is indeed secure.

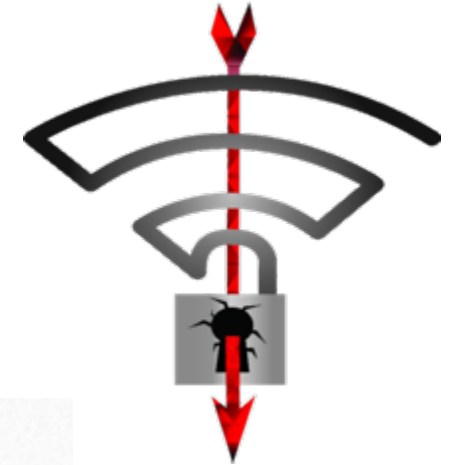
In spite of its history and security proofs though, we show that the 4-way handshake is vulnerable to key reinstallation attacks. Moreover, we discovered similar weaknesses in other Wi-Fi handshakes. That is, we also attack the PeerKey handshake, the group key handshake, and the Fast BSS Transition (FT) handshake.

The idea behind our attacks is rather trivial in hindsight, and can be summarized as follows. When a client joins a network, it executes the 4-way handshake to negotiate a fresh session key. It will install this key after receiving message 3 of the handshake. Once the key

Key Reinstallation Attacks

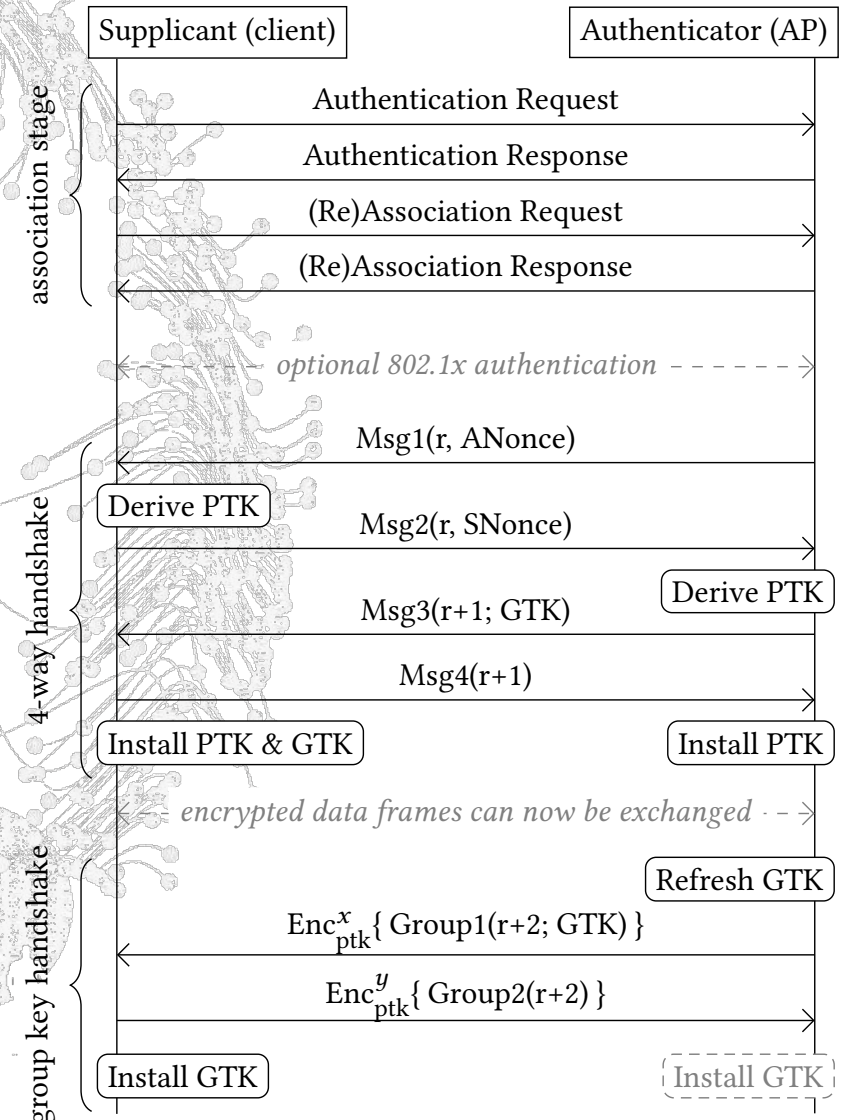
- El 4- way handshake es vulnerable a ataques de reinstalación de clave:
 - Pairwise 4-way handhsake
 - PeerKey handhsake
 - Group Key handshake
 - Fast BSS Transition (FT) Handhsake

- CVE-2017-13077: Reinstallation of the pairwise encryption key (PTK-TK) in the 4-way handshake.
- CVE-2017-13078: Reinstallation of the group key (GTK) in the 4-way handshake.
- CVE-2017-13079: Reinstallation of the integrity group key (IGTK) in the 4-way handshake.
- CVE-2017-13080: Reinstallation of the group key (GTK) in the group key handshake.
- CVE-2017-13081: Reinstallation of the integrity group key (IGTK) in the group key handshake.
- CVE-2017-13082: Accepting a retransmitted Fast BSS Transition (FT) Reassociation Request and reinstalling the pairwise encryption key (PTK-TK) while processing it.
- CVE-2017-13084: Reinstallation of the STK key in the PeerKey handshake.
- CVE-2017-13086: reinstallation of the Tunneled Direct-Link Setup (TDLS) PeerKey (TPK) key in the TDLS handshake.
- CVE-2017-13087: reinstallation of the group key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.
- CVE-2017-13088: reinstallation of the integrity group key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame.



¿Cuál es el problema?

- Cuando un cliente se conecta a una red, ejecuta el 4-way handshake para negociar una nueva clave de sesión
- Instala la clave después de recibir el mensaje 3 que viene del punto de acceso
- Como los paquetes pueden perderse el punto de acceso retransmitirá este 3º mensaje si no ha recibido la correcta confirmación del cliente que viene dada por el mensaje 4
- Como resultado, el cliente recibirá este mensaje 3 varias veces
- Cada vez que reciba este mensaje, reinstalará la misma clave de sesión
- Al reinstalar la clave de sesión, reseteará el nonce y el replay counter utilizados para garantizar la confidencialidad de los datos



¿Cuál es el problema?

- Cuando un cliente se conecta a una red, ejecuta el 4-way handshake para negociar una nueva clave de sesión
- Instala la clave después de recibir el mensaje 3 que viene del punto de acceso
- Como los paquetes pueden perderse el punto de acceso retransmitirá este 3º mensaje si no ha recibido la correcta confirmación del cliente que viene dada por el mensaje 4
- Como resultado , el cliente recibirá este mensaje 3 varias veces
- Cada vez que reciba este mensaje, reinstalará la misma clave de sesión
- Al reinstalar la clave de sesión, reseteará el nonce y el replay counter utilizados para garantizar la confidencialidad de los datos

Impacto dependiente del protocolo de confidencialidad

- Cuando se ataca el 4-way o el Fast Transition handshake el impacto depende del protocolo de confidencialidad utilizado:
 - CCMP → Se pueden descifrar algunos paquetes de manera arbitraria
 - TKIP o GCMP → Se pueden descifrar e inyectar paquetes de manera arbitraria
- Cuando se ataca el group key handshake un atacante puede replicar paquetes broadcast y multicast

All Zero Key

- El impacto del ataque es mayor cuando el cliente utiliza la versión 2.4 o 2.5 del wpa_supplicant.
- En este caso, el cliente no reinstala la clave original, sino una clave con todos los bits a 0 → all_zero key
- Esta vulnerabilidad proviene de una aclaración del estándar 802.11 que sugiere liberar partes de la clave de sesión de memoria una vez que ya ha sido instalada
- Como Android utiliza una versión modificada de wpa_supplicant, todos los dispositivos con Android 6.0 o Android Wear 2.0 tpresentan una vulnerabilidad
- Se calcula que el 31,2% de los dispositivos Android son vulnerables a esta variante crítica del ataque

Aclaraciones

- El ataque no viola las propiedades de seguridad probadas formalmente respecto al 4-way handhsake, considerado como seguro hasta ahora.
- Estas pruebas formales confirman que la clave de cifrado permanece privada y que la identidad tanto de cliente como de AP está confirmada
- Los ataques no revelan la clave de sesión ni la clave de cifrado
- Simplemente, fuerzan a un cliente a reinstalar la clave y con ello resetear los nonce utilizados para garantizar que dos paquetes no se cifran con la misma “keystream”

Fundamento criptográfico

Mensaje Cifrado_1 = Texto_plano_1 XOR F (Clave, **parámetro1**)

Mensaje Cifrado_2 = Texto_plano_2 XOR F(Clave, **parámetro2**)

Mensaje Cifrado_1 = Texto_plano_1 XOR F (Clave, **parámetro**)

Mensaje Cifrado_2 = Texto_plano_2 XOR F(Clave, **parámetro**)

Mensaje Cifrado_1 = Texto_plano_1 XOR **constante**

Mensaje Cifrado_2 = Texto_plano_2 XOR **constante**

Mensaje_Cifrado_1 XOR Mensaje_Cifrado_2 = Texto_plano1 XOR Texto_Plano_2

A = hello
C = secret!

KS= 11010110 00011010 01101011 10001110 11001101 11011111 01001010

A = 01101000 01100101 01101100 01101100 01101111

C = 01110011 01100101 01100011 01110010 01100101 01110100 00100001

B = 10111110 01111111 00000111 11100010 10100010

D = 10100101 01111111 00001000 11111100 10101000 10101011 01101011

Algunos detalles

- Debido a que Windows e iOS no han seguido el estándar 802.11 al pie de la letra, no aceptan la retransmisión del 3º mensaje del handshake por lo que no son vulnerables a este ataque.
- No obstante, lo son a la reinstalación de la clave de grupo o al BSS Fast Transition Handshake por parte del AP
- Respecto a los puntos de acceso, sólo aquellos que soportan 802.11r son vulnerables al BSS FT Handshake.
- Típicamente puntos de acceso utilizados en el ámbito corporativo.

Implementation	Re. Msg3	Pt. EAPOL	Quick Pt.	Quick Ct.	4-way	Group
OS X 10.9.5	✓	✗	✗	✓	✓	✓
macOS Sierra 10.12	✓	✗	✗	✓	✓	✓
iOS 10.3.1 ^c	✗	N/A	N/A	N/A	✗	✓
wpa_supplicant v2.3	✓	✓	✓	✓	✓	✓
wpa_supplicant v2.4-5	✓	✓	✓	✓ ^a	✓ ^a	✓
wpa_supplicant v2.6	✓	✓	✓	✓ ^b	✓ ^b	✓
Android 6.0.1	✓	✗	✓	✓ ^a	✓ ^a	✓
OpenBSD 6.1 (rum)	✓	✗	✗	✗	✗	✓
OpenBSD 6.1 (iwn)	✓	✗	✗	✓	✓	✓
Windows 7 ^c	✗	N/A	N/A	N/A	✗	✓
Windows 10 ^c	✗	N/A	N/A	N/A	✗	✓
MediaTek	✓	✓	✓	✓	✓	✓

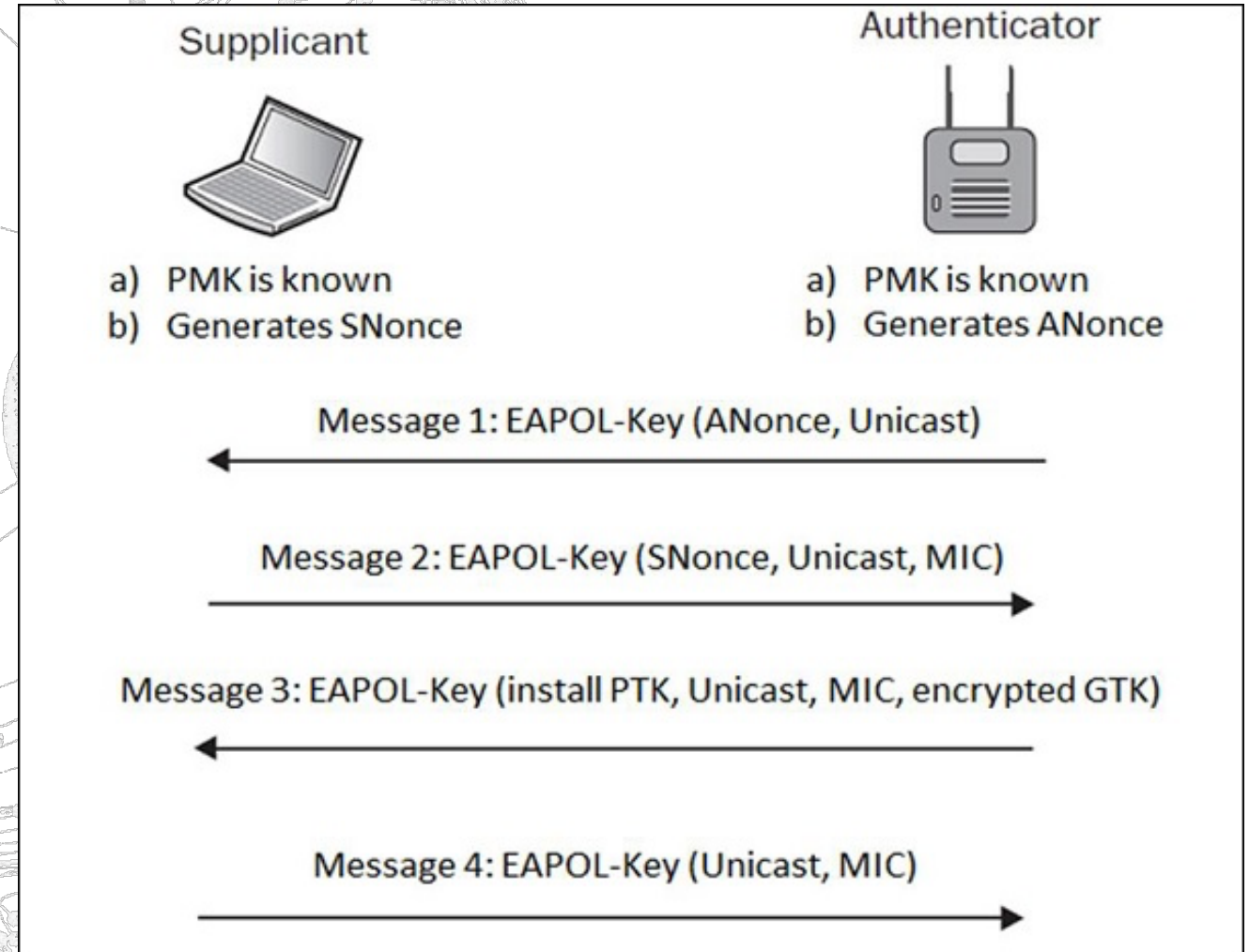
^a Due to a bug, an all-zero TK will be installed, see Section 6.3.

^b Only the group key is reinstalled in the 4-way handshake.

^c Certain tests are irrelevant (not applicable) because the implementation does not accept retransmissions of message 3.

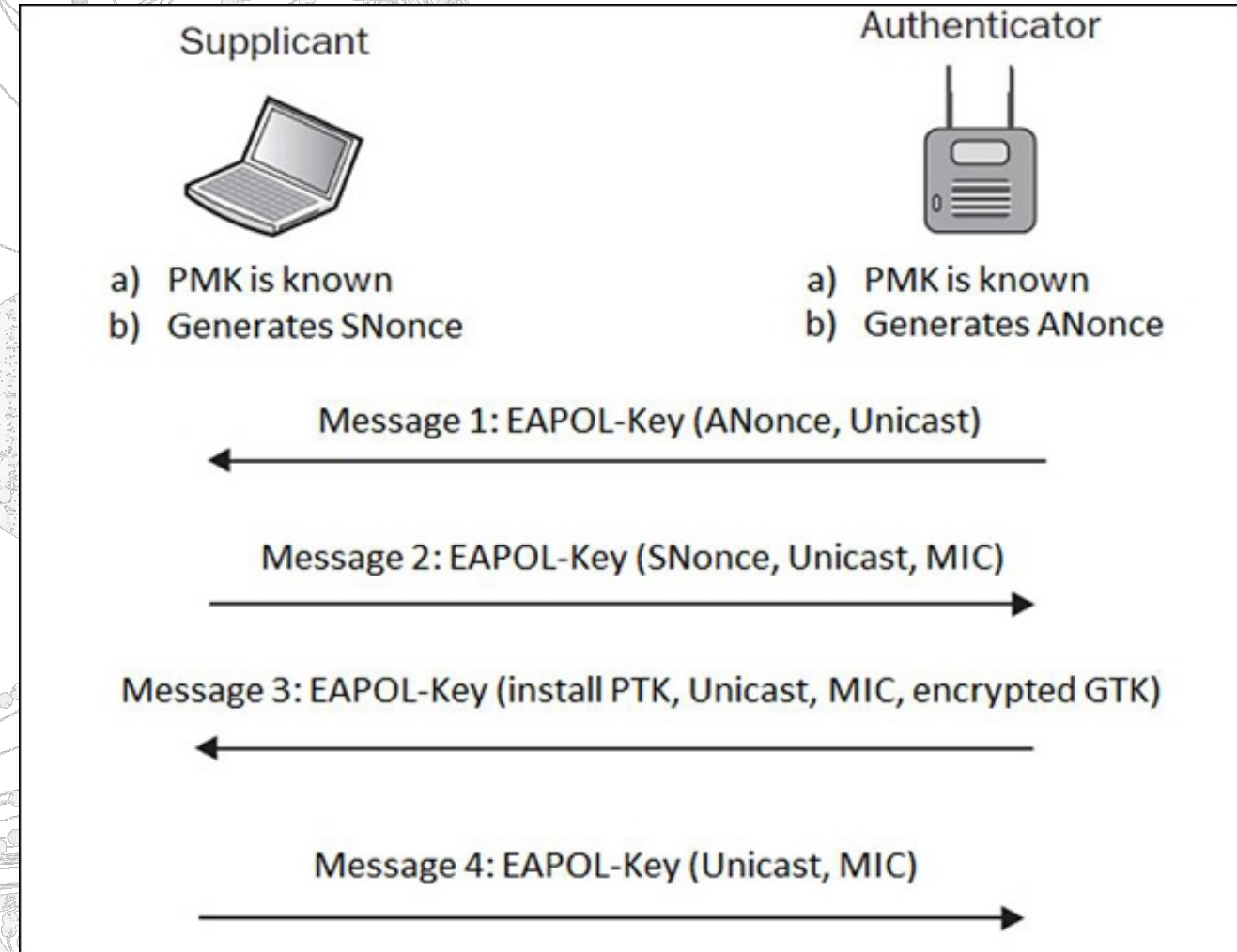
4 Way Handshake

- La Pairwise Master Key se conoce
- Se genera a partir del SSID y la PSK
- La Pairwise-Transient-Keys PTK se genera a partir de:
 - La PMK
 - Dirección MAC del cliente
 - Dirección MAC del punto de acceso
 - Nonce del punto de acceso (ANonce)
 - Nonce del cliente (Snonce)

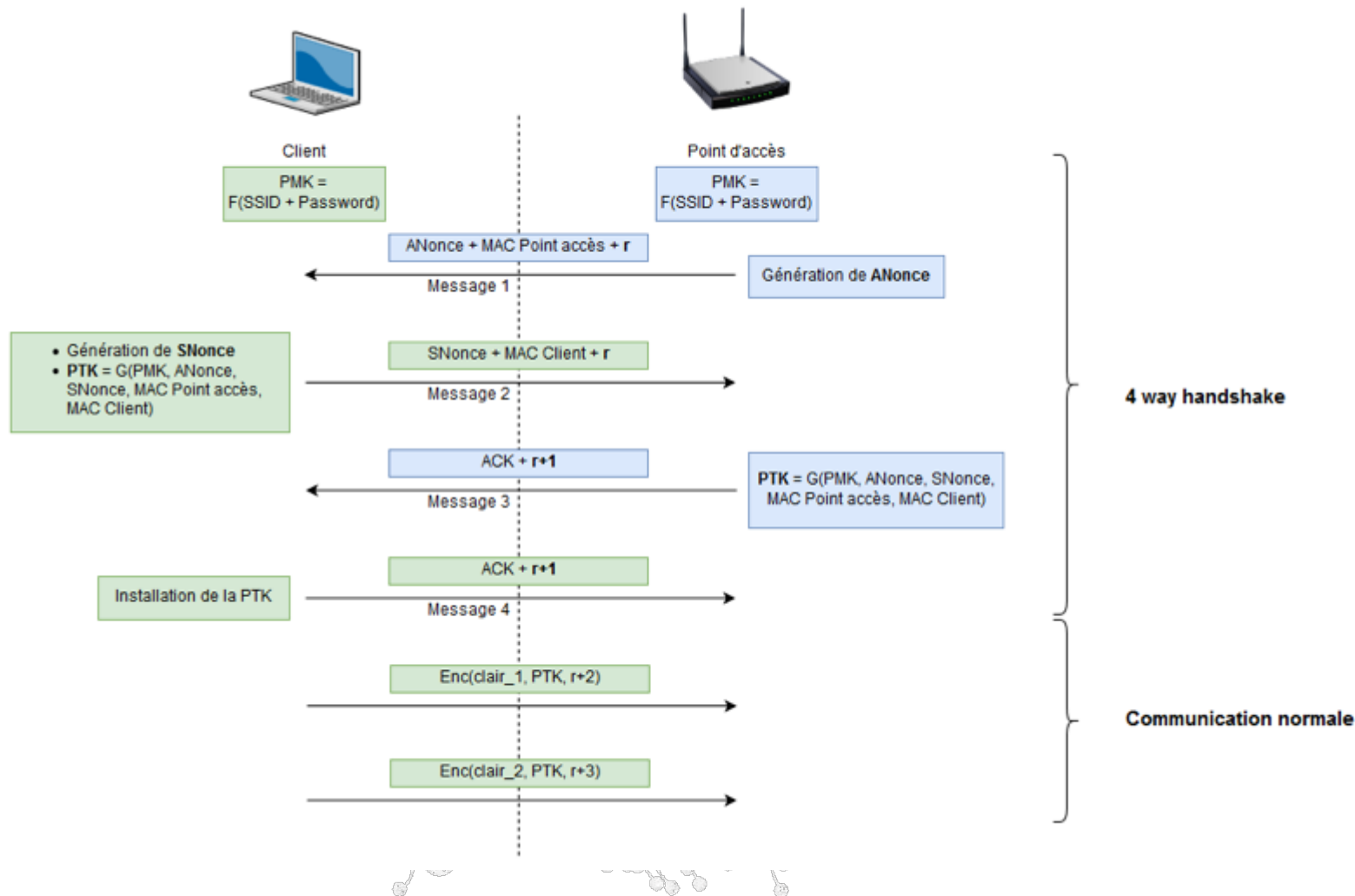


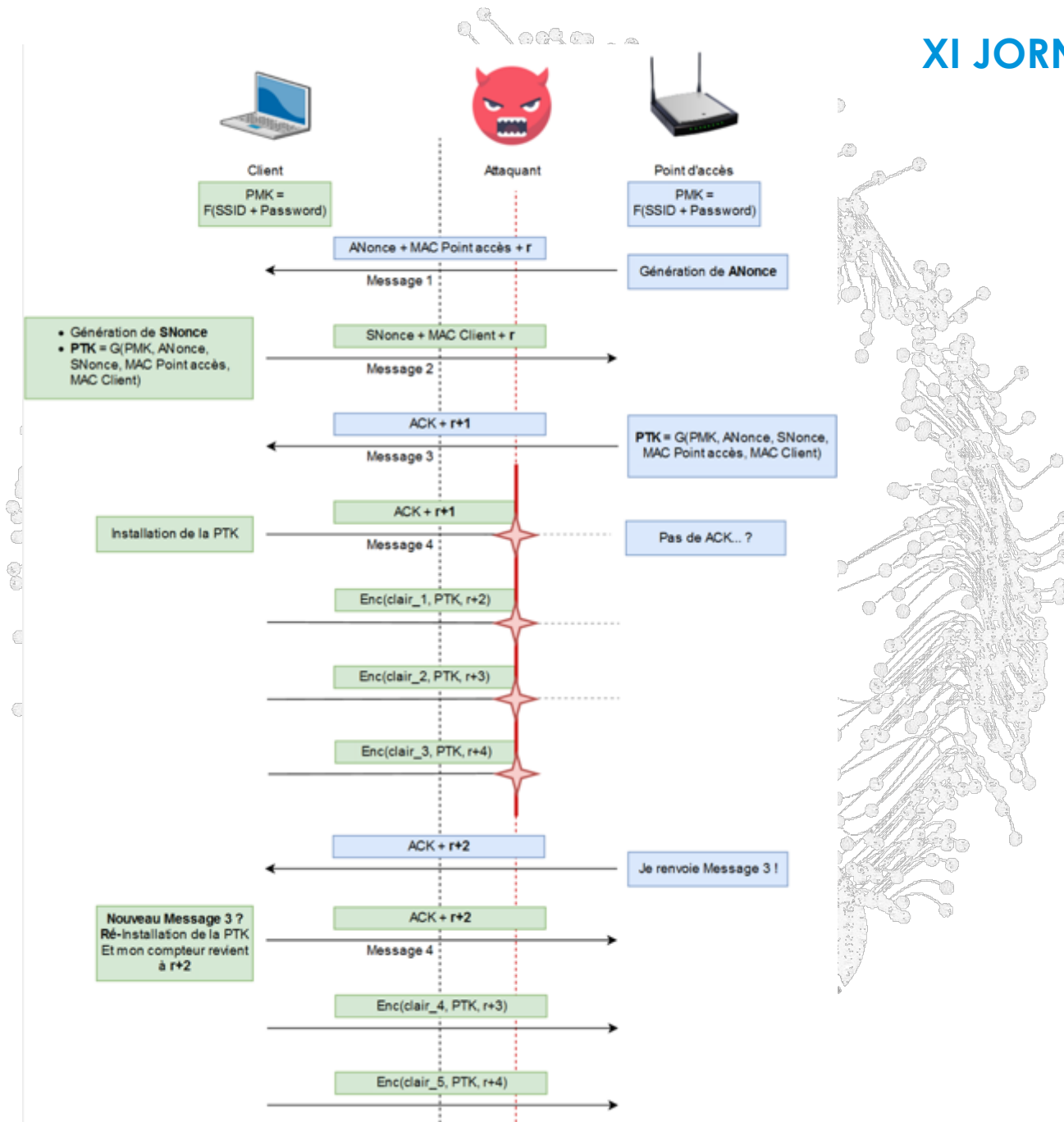
4 Way Handshake

- La Pairwise-Transient-Keys PTK se compone de:
 - Key Confirmation Key (KCK) usada durante la creación del MIC (128 bits)
 - Key Encryption Key: (KEK) Usada por el punto de acceso durante el cifrado (128 bits)
 - Temporal Key (TK):** Clave de cifrado utilizada para cifrar y descifrar los paquetes unicast (128 bits)
 - Mic Authenticator TX Key (MIC Tx): Usada con TKIP para paquetes unicast enviados por puntos de acceso (64 bits)
 - MIC Authenticator Rx usada con TKIP para paquetes enviados por clientes (64 bits)

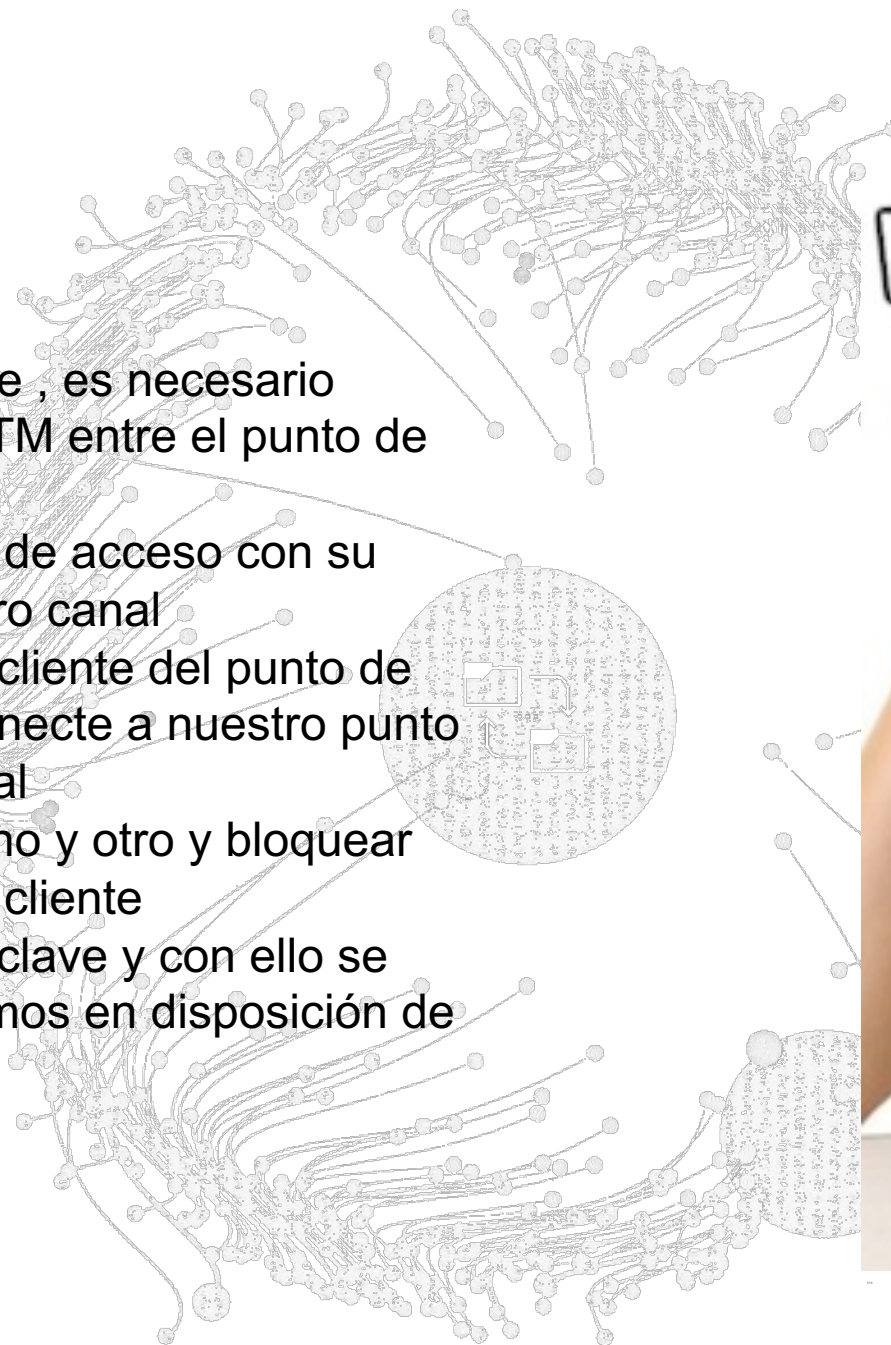


4 Way Handshake





- Para poder replicar el ataque , es necesario hacer un channel-based MITM entre el punto de acceso y el cliente
- Se ha de suplantar al punto de acceso con su misma dirección MAC en otro canal
- Conseguir “deautenticar” al cliente del punto de acceso legítimo y se que conecte a nuestro punto de acceso falso en otro canal
- Enviar los paquetes entre uno y otro y bloquear el mensaje 4 enviado por el cliente
- Una vez que se reinstale la clave y con ello se reseteen los nonces estaremos en disposición de poder descifrar el tráfico



**WHAT BUTTON DO I
PRESS**

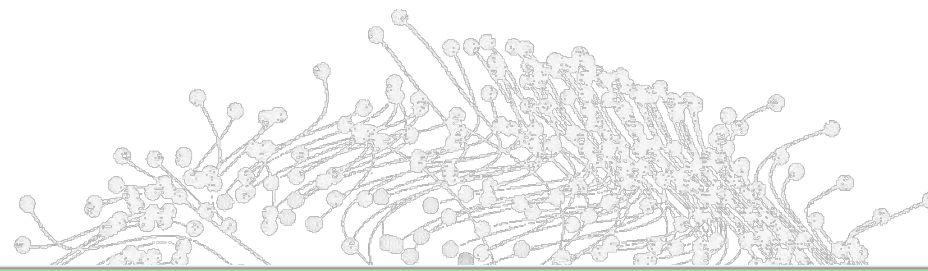
**TO HACK
SOMEONE?**



wlan.sa == 38:94:96:95:73:77 && wlan.ccmp.extiv == "0x000000000007"

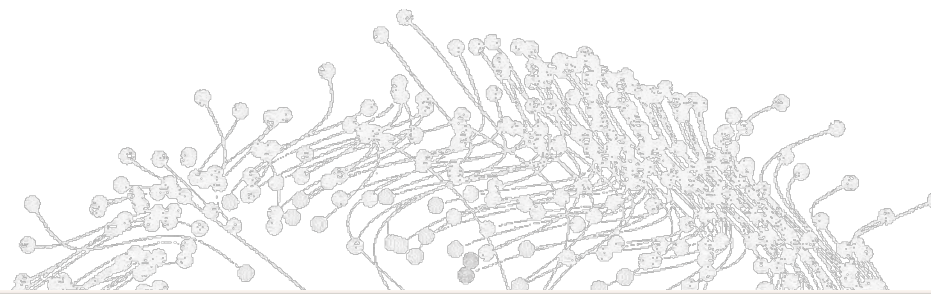
No.	Time	Source	Destination	Protocol	Length	Info
75	6.641543	192.168.1.39	80.58.61.254	DNS	125	Standard query 0x2291 A connectivitycheck.gstatic.com

Receiver address: D-LinkIn_35:13:cb (80:26:89:35:13:cb)
 Destination address: Mitrasta_b1:cc:56 (34:57:60:b1:cc:56)
 Transmitter address: SamsungE_95:73:77 (38:94:96:95:73:77)
 Source address: SamsungE_95:73:77 (38:94:96:95:73:77)
 BSS Id: D-LinkIn_35:13:cb (80:26:89:35:13:cb)
 STA address: SamsungE_95:73:77 (38:94:96:95:73:77)
 0000 = Fragment number: 0
 0000 0000 0110 = Sequence number: 6
 ▶ Qos Control: 0x0000
 ▼ CCMP parameters
 CCMP Ext. Initialization Vector: 0x000000000007
 Key Index: 0



wlan.sa == 38:94:96:95:73:77 && wlan.ccmp.extiv == "0x00000000000008"						
No.	Time	Source	Destination	Protocol	Length	Info
77	6.642568	192.168.1.39	80.58.61.250	DNS	125	Standard query 0x116f A connectivitycheck.gstatic.com
Receiver address: D-LinkIn_35:13:cb (80:26:89:35:13:cb) Destination address: Mitrasta_b1:cc:56 (34:57:60:b1:cc:56) Transmitter address: SamsungE_95:73:77 (38:94:96:95:73:77) Source address: SamsungE_95:73:77 (38:94:96:95:73:77) BSS Id: D-LinkIn_35:13:cb (80:26:89:35:13:cb) STA address: SamsungE_95:73:77 (38:94:96:95:73:77) 0000 = Fragment number: 0 0000 0000 0111 = Sequence number: 7 ▶ Qos Control: 0x0000 ▼ CCMP parameters CCMP Ext. Initialization Vector: 0x00000000000008 Key Index: 0						

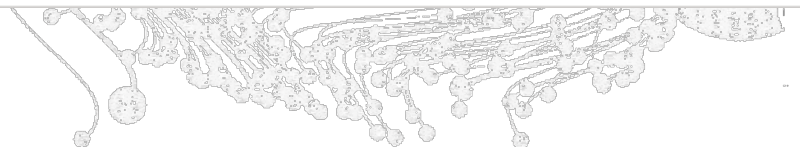




wlan.da == c6:ea:3f:d0:e3:3d && wlan.sa == 38:94:96:95:73:77 && wlan.ccmp.extiv == "0x000000000002"

No.	Time	Source	Destination	Protocol	Length	Info
345	20.223842314	192.168.100.2	192.168.100.254	DNS	165	Standard query 0x9ee5 A connectivitycheck.gstatic.com
396	23.411753828	192.168.100.2	192.168.100.254	DNS	165	Standard query 0xdfbb A connectivitycheck.gstatic.com
430	25.178230018	192.168.100.2	192.168.100.254	DNS	168	Standard query 0xa64d A mtalk.google.com.krackattack.com
465	26.583145250	SamsungE_95:73:77	c6:ea:3f:d0:e3:3d	ARP	118	192.168.100.2 is at 38:94:96:95:73:77
541	30.061094720	SamsungE_95:73:77	c6:ea:3f:d0:e3:3d	EAPOL	189	Key (Message 4 of 4)
548	30.318909707	SamsungE_95:73:77	c6:ea:3f:d0:e3:3d	ARP	118	192.168.100.2 is at 38:94:96:95:73:77
609	34.054082152	SamsungE_95:73:77	c6:ea:3f:d0:e3:3d	EAPOL	189	Key (Message 4 of 4)
627	35.208349080	SamsungE_95:73:77	c6:ea:3f:d0:e3:3d	ARP	118	Who has 192.168.100.254? Tell 192.168.100.2
664	36.605263780	192.168.100.2	192.168.100.254	DNS	165	Standard query 0xaa77 A connectivitycheck.gstatic.com
735	39.999250161	SamsungE_95:73:77	c6:ea:3f:d0:e3:3d	EAPOL	189	Key (Message 4 of 4)
824	46.141756351	SamsungE_95:73:77	c6:ea:3f:d0:e3:3d	EAPOL	189	Key (Message 4 of 4)

Transmitter address: SamsungE_95:73:77 (38:94:96:95:73:77)
Source address: SamsungE_95:73:77 (38:94:96:95:73:77)
BSS Id: c6:ea:3f:d0:e3:3d (c6:ea:3f:d0:e3:3d)
STA address: SamsungE_95:73:77 (38:94:96:95:73:77)
.... 0000 = Fragment number: 0
0000 0000 1110 = Sequence number: 14
Frame check sequence: 0x234e082e [correct]
[FCS Status: Good]
► Qos Control: 0x0006
▼ CCMP parameters
CCMP Ext. Initialization Vector: 0x000000000002
Key Index: 0



Vendor	Patch Available	In Development	Not Directly Affected
Apple	X	?	
Arch Linux	X		
Arista			X
Aruba	X		
Asus		X	X
CentOS	X		
Cisco	X		
DD-WRT	X		
Debian	X		
Endian	X		
Extreme Networks	X	X	
Fedora	X		
FreeBSD	X		
Google	X		
Lenovo			?
LineageOS	X		
LXDE		X	
Meraki	X		
MikroTik	X		
Mojo Networks	X		
Red Hat	X		
Ruckus	X		
Synology	X		

Conclusiones

- La vulnerabilidad descubierta por Mathy Vanhoef demuestra que efectivamente el tráfico WPA2 puede ser descifrado sin conocer la clave de cifrado de la red, dependiendo de las circunstancias
- El ataque es plausible pero requiere de ciertas condiciones para poder ser llevado a cabo
- De momento no existe herramienta de botón gordo que lo reproduzca
- Prácticamente todos los dispositivos son vulnerables a alguno de los ataques
- Estar alerta de las actualizaciones de los fabricantes tanto para puntos de acceso como para dispositivos cliente



¡¡ Muchas gracias a la organización y asistentes !!

➤ E-Mails

- info@ccn-cert.cni.es
- ccn@cni.es
- sat-inet@ccn-cert.cni.es
- sat-sara@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es

➤ Síguenos en

