Pero… ¡mi estación está despierta!
Denegación de servicio basado en Power Save en redes Wi-Fi (IEEE 802.11)

Leandro F. Meiners

lea@coresecurity.com

Agenda

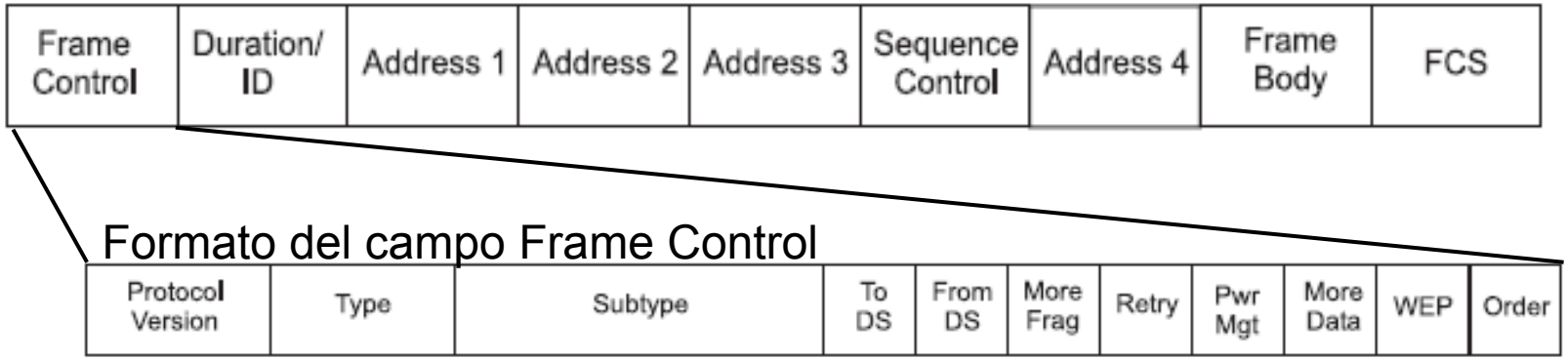
- **Tramas en IEEE 802.11**
  - Clases y formatos de tramas
  - Bit de power management
- **Mecanismo de ahorro de energía (power save) en IEEE 802.11**
- **Motivación del ataque**
- **Funcionamiento del ataque de denegación de servicio**
  - Tramas candidatas
  - Pseudo-código del ataque
- **Contramedidas/Mitigación**

- Clases de tramas MAC en IEEE 802.11:
  - Gestión (management): utilizados para el manejo de la red, por ejemplo la asociación de estaciones a la misma.
  - Control: utilizados para regular el acceso al medio, por ejemplo confirmaciones de recepción de datos.
  - Datos: utilizados para el envío de datos de capa superiores. Al utilizar WEP/WPA/WPA2 únicamente éstas tramas están cifradas.

- Algunas tramas que nos interesan…

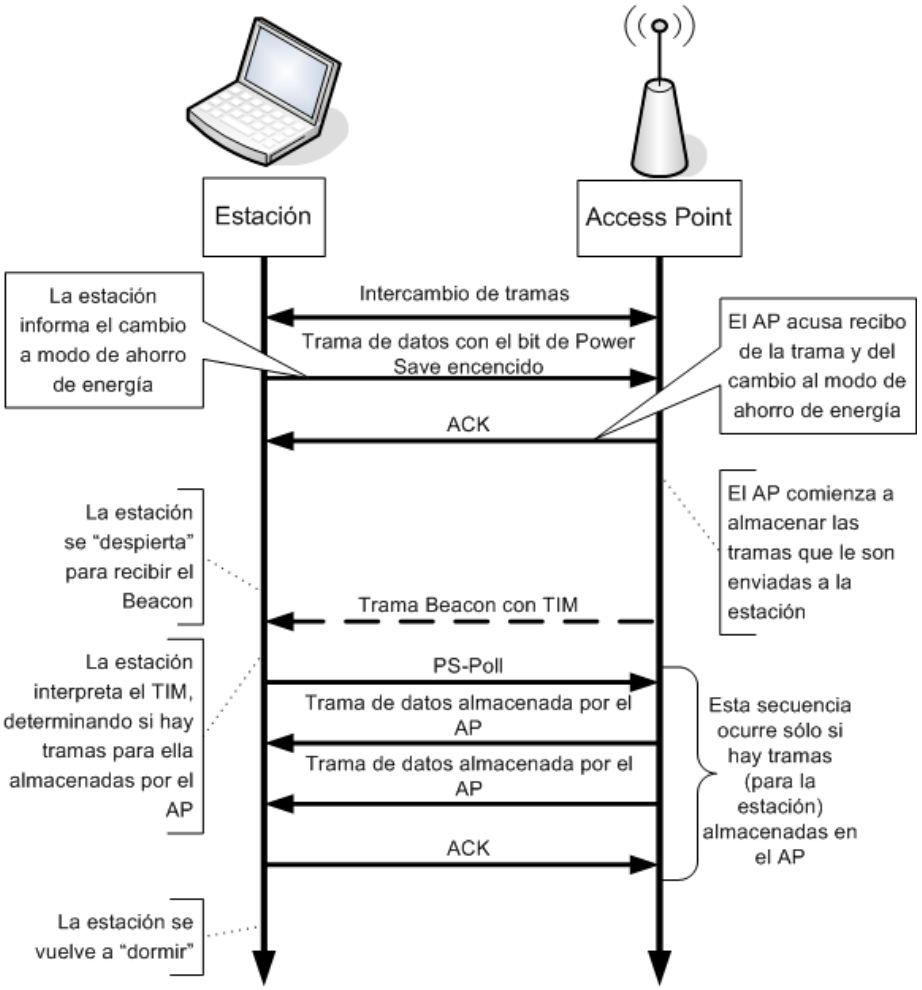
Tipo de Trama	Subtipo	Descripción/Uso
Gestión	Reassociation Request (Pedido de reasociación)	Pedido de reasociación a la red, utilizado, por ejemplo, al cambiar de AP dentro de la misma red
Gestión	Beacon (baliza)	Indica la presencia y capacidades de un AP
Gestión	Probe Request (sonda)	Consulta la existencia/disponibilidad de una red
Control	RTS (request to send)	Pedido de envío de tramas (reserva del medio físico)
Control	PS-Poll	Utilizado por una estación en modo de ahorro de energía para solicitar las tramas pendientes almacenadas por el AP
Datos	Null Function (no data)	Trama de datos vacía

Formato de la trama MAC



- Power Management Bit (parte del campo Frame Control):
  - Indica el modo de power management que la estación transmisora adoptará luego de la secuencia actual de intercambio de tramas.
  - Debe permanecer constante durante una secuencia de intercambio de tramas.
  - = 1 ⇒ ahorro de energía
  - = 0 ⇒ activo

Mecanismo de Power Save



- **Propiedades de la funcionalidad de Power Save:**
  - Una estación permanece en el modo actual de power-management hasta que le informa del cambio al AP a través de cualquier intercambio de tramas.
  - TIM (Traffic Indication Map):
    - » Indica que estaciones tienen tramas almacenadas por el AP
    - » Contenido en las tramas Beacon

11.2.1 Power management in an infrastructure network

STAs changing Power Management mode shall inform the AP of this fact using the Power Management bits within the Frame Control field of transmitted frames. The AP shall not arbitrarily transmit MSDUs to STAs operating in a PS mode, but shall buffer MSDUs and only transmit them at designated times.

¿Posible DoS?

Vocabulario:

STA: estación **AP**: Access point

MSDU: forma pomposa de decir trama

PS: Power-save

...

A STA shall remain in its current Power Management mode until it informs the AP of a Power Management mode change via a frame exchange that includes an acknowledgment from the AP. Power Management mode shall not change during any single frame exchange sequence, as described in 9.12.

Y, si engaño al AP para que piense que la estación está en power-save…

¿cómo se entera la estación de este cambio?

11.2.1 Power management in an infrastructure network

…

The STAs that currently have buffered MSDUs within the AP are identified in a TIM, which shall be included as an element within all Beacon frames generated by the AP. A STA shall determine that an MSDU is buffered for it by receiving and interpreting a TIM.

Entonces… el beacon indica que hay tramas almacenadas

Vocabulario:

STA: estación **AP**: Access point

MSDU: forma pomposa de decir trama

TIM: indica que estaciones tienen tramas almacenadas por el AP

PS: Power-save

…

STAs operating in PS modes shall periodically listen for Beacon frames, as determined by the STA's ListenInterval and the ReceiveDTIMs parameter in the MLME-POWERMGT.request primitive.

Y, las estaciones en PS lo interpretan…

¿Y las estaciones activas?

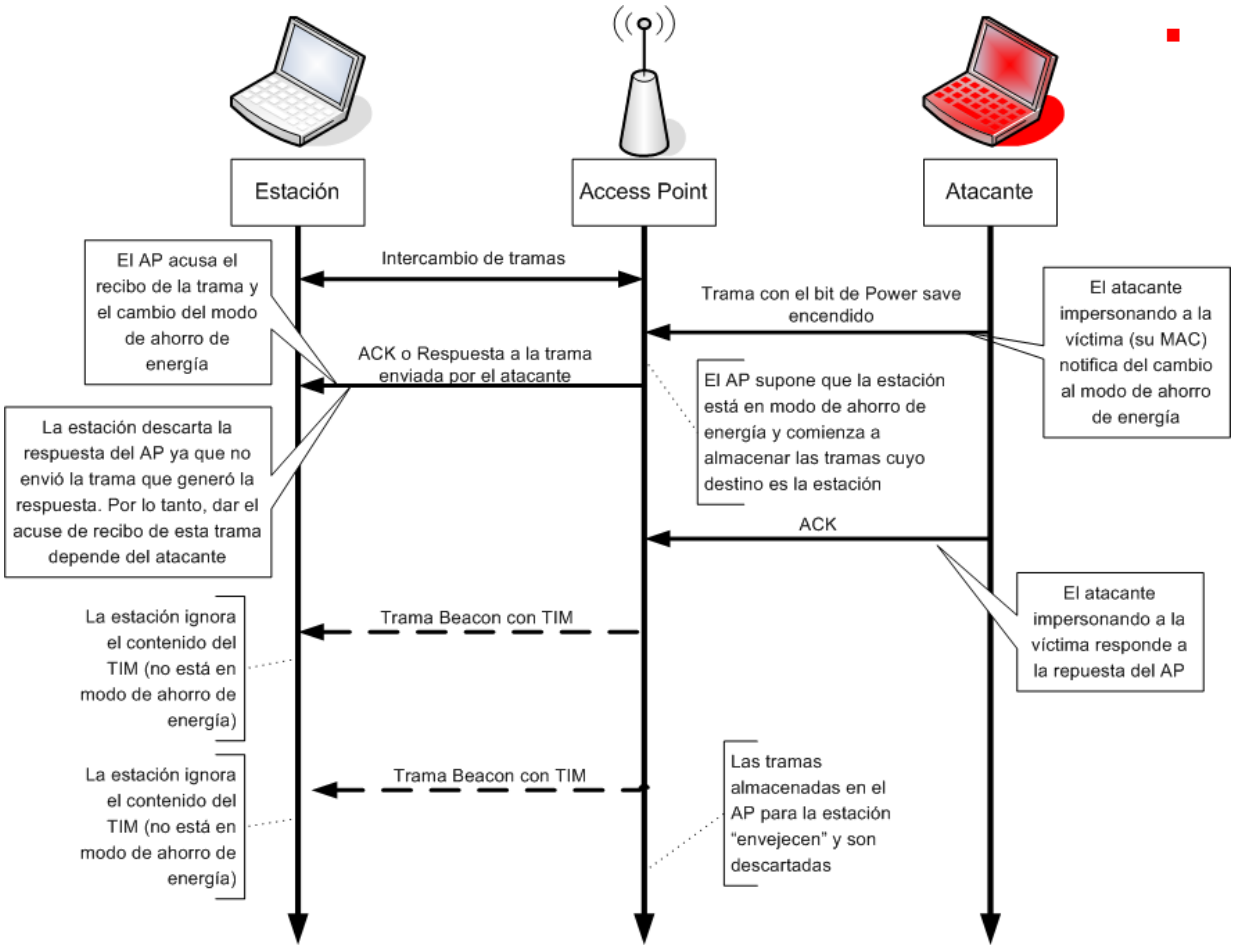
11.2.1.10 STAs operating in the Active mode

A STA operating in this mode shall have its receiver activated continuously; such STAs do not need to interpret the TIM information elements in Beacon frames.

...

An AP shall have an aging function to delete pending traffic buffered for an excessive time period. The exact specification of the aging function is beyond the scope of this standard.

Funcionamiento del ataque



- **Propiedades del ataque:**
  - Escaso uso de ancho de banda (una trama por cada intercambio de tramas enviado por la estación víctima).
  - Es específico (permite definir las estaciones víctimas).
  - Debido al bajo consumo de ancho de banda es posible atacar múltiples estaciones al mismo tiempo.

- **Propiedades de las tramas candidatas:**
  - Idealmente, no debería requerir conocer la clave de cifrado (por si la red utiliza WEP/WPA/WPA2). Esto limita las posibilidades sólo a tramas de *gestión*, *control* o de “null function” (datos vacía).
  - El estándar prohíbe realizar un cambio de estado del modo de ahorro de energía durante una secuencia de tramas, luego debemos encontrar una secuencia lo más corta:
    - » Así evitar que la estación víctima envíe datos en el ínterin, que puedan anular el ataque
    - » Disminuye la carga de trabajo por parte del atacante que debe realizar toda la secuencia

- **Posibles tramas:**
  - Request to Send (RTS): generalmente descartados por los AP
  - Reassociation Request (Pedido de reasociación)
  - Probe Request (sonda)
  - **Null Function (no data)**

- **La revisión IEEE 802.11-2007 agrega “The Power Managment bit shall not be set in any management frame, except an Action frame.”**

Pseudocódigo del ataque


```
# Generamos la trama para cambiar a modo de ahorro de energía
trama_DoS = trama_80211(src_mac='MACVictima', dst_mac='BSSID', PowerBit=1)
trama_DoS.setType('Data')
trama_DoS.setSubType('NullFunction')

# Generamos una trama ACK (por si debemos enviar un acuse de recibo)
trama_ACK = trama_ACK_80211(ra_mac='BSSID')

start_sniffer()

send(trama_DoS)
while True:
        trama = sniff_next_frame()
        # Si la víctima genera tráfico el AP concluye un cambio
        # de estado, debemos volver a cambiarlo a power save (PS)
        if ( srcMac(trama)=='MACVictima' && pwrMgmt(trama)==0 ):
                send(trama_DoS)

        # Si el AP le envía datos a la vícitma, o bien es una respuesta
        # a la trama DoS (en cuyo caso solo mandamos un acuse de recibo)
        # o el AP no interpretó el cambio de estado a PS, reintentamos
        if ( srcMac(trama)=='BSSID' && dstMAC(trama)=='MACVictima' ):
                if( subtype(trama).isResponse(subtype(trama_DoS)) ):
                        send(trama_ACK)
                else
                        send(trama_DoS)
```

- **Contramedidas:**
  - El ataque es posible debido al robo de “identidad” de la estación víctima. De modificar el estándar para que **todas** las tramas estén autenticadas (y no únicamente las tramas de datos), se resolvería los problemas basados en el robo de “identidad” (MAC spoofing).

- **Mitigaciones:**
  - Eliminar todas las tramas candidatas para realizar el ataque:
    - » Si los AP únicamente procesan cambios en el modo de ahorro de energía en tramas de datos (no vacías), en redes con WPA/WPA2, debido a la autenticación y protección contra ataques de replay que ofrece para tramas de datos, el ataque se vería mitigado.
  - Forzar la resincronización entre la víctima y el AP:
    - » Si la estación interpreta el TIM aún estando activa y, de ser necesario, envía un PS-Poll, la única consecuencia del ataque es la demora en la recepción de tramas.

- **Modificación a los drivers rt2570**

```
--- rt2570-cvs-20080604l3/Module/sync.c 2008-04-27 16:06:47.000000000 -0300
+++ rt2570-cvs-20080604l3-PS-DoS-Fix/Module/sync.c      2008-06-05 17:07:50.000000000 -0300
@@ -973,6 +973,13 @@
                    ULONG   PowerMode;
                        PowerMode = pAd->PortCfg.WindowsPowerMode;

+                   /* Still send PSPoll if we have buffered frames even though we are not is PWR_SAVE mode */
+                   if (MessageToMe)
+                   {
+                       DBGPRINT(RT_DEBUG_TRACE, "SYNC - AP backlog, we are AWAKE so we stay AWAKE but send PSPOLL\n");
+                       EnqueuePsPoll(pAd);
+                   }
+
                    if ((PowerMode != Ndis802_11PowerModeCAM) &&
                        (pAd->BulkOutPending == FALSE) &&
                        (!LOCAL_TX_RING_EMPTY(pAd)) &&
```

- Ventajas de la mitigación:
  - No requiere modificar el firmware de los AP
  - Es backward compatible con implementaciones actuales (pueden coexistir estaciones con y sin el “parche” en la misma red)
  - Independiente del mecanismo de cifrado soportado por la red

Preguntas

http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=publication&name=WiFi_Power_Save_DoS

lea@coresecurity.com