# *Pruebas de Seguridad en implementaciones 802.11k/v*

Trabajo Final de Master

Javier Contreras Albesa
MISTIC - UOC

# Agenda

- Introducción
- Objetivos
- Método
- Laboratorio
- Pruebas Realizadas
- Resultados
- Demo

# Introducción

# Introducción

- Redes WiFi
  - 7.000 Millones de dispositivos en 2017
- 802.11-2012
  - Optimizaciones para el Roaming
- 802.11k
  - Mecanismos para la medición de recursos de radio
- 802.11v
  - Gestión de red inalámbrica, topologia, transición
- 802.11r
  - Roaming rápido y seguro entre puntos de acceso

# Inicio de una Propuesta

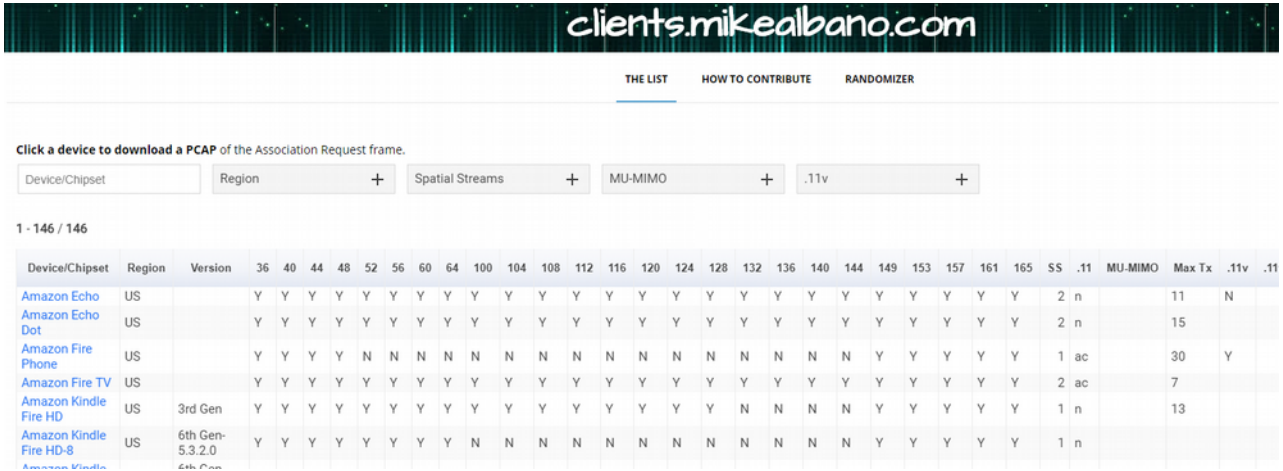
- Uso de 802.11k/v como vector de ataque
- Reacción de dispositivos a mensajes 802.11k/v manipulados
- Fuzz de mensajes 802.11k/v
- Actual carencia de herramientas para validación

- -> Creación de nueva Herramienta!

# Objetivos

# Que hay que hacer?

- Selección de Dispositivos a Evaluar



clients.mikealbano.com

THE LIST HOW TO CONTRIBUTE RANDOMIZER

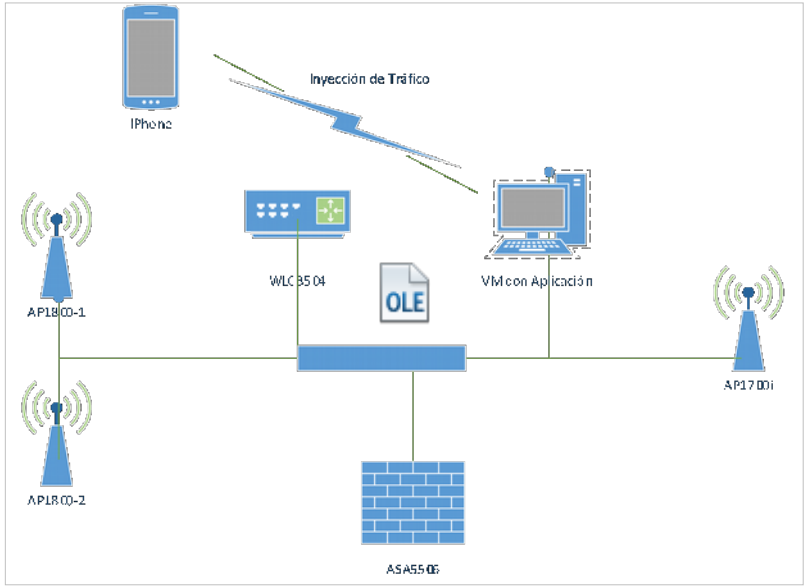
**Click a device to download a PCAP** of the Association Request frame.

Device/Chipset | Region + | Spatial Streams + | MU-MIMO + | .11v +

1 - 146 / 146

| Device/Chipset | Region | Version | 36 | 40 | 44 | 48 | 52 | 56 | 60 | 64 | 100 | 104 | 108 | 112 | 116 | 120 | 124 | 128 | 132 | 136 | 140 | 144 | 149 | 153 | 157 | 161 | 165 | SS | .11 | MU-MIMO | Max Tx | .11v | .11 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Amazon Echo | US | | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | 2 | n | | 11 | N | |
| Amazon Echo Dot | US | | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | 2 | n | | 15 | | |
| Amazon Fire Phone | US | | Y | Y | Y | Y | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | 1 | ac | | 30 | Y | |
| Amazon Fire TV | US | | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | 2 | ac | | 7 | | |
| Amazon Kindle Fire HD | US | 3rd Gen | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | Y | N | N | N | N | Y | Y | Y | Y | Y | 1 | n | | 13 | | |
| Amazon Kindle Fire HD-8 | US | 6th Gen-5.3.2.0 | Y | Y | Y | Y | Y | Y | Y | Y | N | N | N | N | N | N | N | N | N | N | N | N | Y | Y | Y | Y | Y | 1 | n | | | | |
| Amazon Kindle | | 6th Gen | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

# El Laboratorio




# Que hay que hacer?

- Comprobación de los clientes

```
> Tag: Power Capability Min: 249, Max :19
> Tag: Supported Channels
> Tag: RSN Information
v Tag: RM Enabled Capabilities (5 octets)
    Tag Number: RM Enabled Capabilities (70)
    Tag length: 5
  > RM Capabilities: 0x30 (octet 1)
  > RM Capabilities: 0x08 (octet 2)
  v RM Capabilities: 0x01 (octet 3)
      .... ...1 = AP Channel Report capability: Enabled
      .... ..0. = RM MIB capability: Disabled
      ...0 00.. = Operating Channel Max Measurement Duration: 0
      000. .... = Nonoperating Channel Max Measurement Duration: 0
  v RM Capabilities: 0x00 (octet 4)
      .... .000 = Measurement Pilotcapability: 0
      .... 0... = Measurement Pilot Transmission Information: Disabled
      ...0 .... = Neighbor Report TSF Offset: Disabled
```

Iphone7 11k

Iphone7 11v

```
> Tag: RM Enabled Capabilities (5 octets)
> Tag: Mobility Domain
> Tag: HT Capabilities (802.11n D1.10)
v Tag: Extended Capabilities (3 octets)
    Tag Number: Extended Capabilities (127)
    Tag length: 3
  > Extended Capabilities: 0x00 (octet 1)
  > Extended Capabilities: 0x00 (octet 2)
  v Extended Capabilities: 0x08 (octet 3)
      .... ...0 = TFS: Not supported
      .... ..0. = WNM-Sleep Mode: Not supported
      .... .0.. = TIM Broadcast: Not supported
      .... 1... = BSS Transition: Supported
      ...0 .... = QoS Traffic Capability: Not support
      ..0. .... = AC Station Count: Not supported
      .0.. .... = Multiple BSSID: Not supported
      0... .... = Timing Measurement: Not supported
```

# Que hay que hacer?

- Comprobación de los clientes +

```
Tag: RM Enabled Capabilities (5 octets)
    Tag Number: RM Enabled Capabilities (70)
    Tag length: 5
  RM Capabilities: 0x73 (octet 1)
      .... ...1 = Link Measurement: Enabled
      .... ..1. = Neighbor Report: Enabled
      .... .0.. = Parallel Measurements: Disabled
      .... 0... = Repeated Measurements: Disabled
      ...1 .... = Beacon Passive Measurement: Enabled
      ..1. .... = Beacon Active Measurement: Enabled
      .1.. .... = Beacon Table Measurement: Supported
      0... .... = Beacon Measurement Reporting Conditions: Disabled
```

Samsung S7 11k

Samsung S7 11v

```
  RM Capabilities: 0x73 (octet 1)
  RM Capabilities: 0x08 (octet 2)
  RM Capabilities: 0x01 (octet 3)
      .... ...1 = AP Channel Report capability: Enabled
      .... ..0. = RM MIB capability: Disabled
      ...0 00.. = Operating Channel Max Measurement Duration: 0
      000. .... = Nonoperating Channel Max Measurement Duration: 0
  RM Capabilities: 0x00 (octet 4)
  RM Capabilities: 0x00 (octet 5)
Tag: HT Capabilities (802.11n D1.10)
Tag: Extended Capabilities (8 octets)
Tag: VHT Capabilities (IEEE Std 802.11ac/D3.1)
```

# Captura de Tramas

- Actividad 11k/v realizada por los clientes/APs

```
802.11 radio information
IEEE 802.11 Action, Flags: ........C
IEEE 802.11 wireless LAN management frame
  Fixed parameters
      Category code: Radio Measurement (5)
      Action code: Neighbor Report Request (4)
      Dialog token: 1
  Tagged parameters (7 bytes)
    Tag: SSID parameter set: home1
        Tag Number: SSID parameter set (0)
        Tag length: 5
        SSID: home1
```

Petición de Vecinos

Respuesta de Vecinos

```
IEEE 802.11 wireless LAN management frame
  Fixed parameters
     Category code: Radio Measurement (5)
     Action code: Neighbor Report Response (5)
     Dialog token: 8
  Tagged parameters (60 bytes)
    Tag: Neighbor Report
       Tag Number: Neighbor Report (52)
       Tag length: 13
       BSSID: Cisco_0d:56:af (0c:75:bd:0d:56:af)
     > BSSID Information: 0x000002f7
       Operating Class: 0
       Channel Number: 40 (iterative measurements on that Channel Number)
       PHY Type: 0x07
    > Tag: Neighbor Report
```

# Captura de Tramas

- Actividad 11k/v realizada por los clientes/APs

Reporte de Medición

```
Tag: Measurement Report
    Tag Number: Measurement Report (39)
    Tag length: 29
    Measurement Token: 0x60
  Measurement Report Mode: 0x00
      .... ...0 = Measurement Report Mode Field: Disabled
      .... ..0. = Measurement Reports: Not Accepted
      .... .0.. = Autonomous Measurement Reports: Not Accepted
      0000 0... = Reserved: 0x00
  Measurement Report Type: Beacon Report (0x05)
      Operating Class: 241
      Measurement Channel Number: 40 (iterative measurements on that Channel Number)
      Measurement Start Time: 0x46214628300ef88d
      Measurement Duration: 0xbcb3
    Reported Frame Information: 0x00
      Received Channel Power Indicator (RCPI): 0xd6
      Received Signal to Noise Indicator (RSNI): 0x23
      BSSID Being Reported: Cisco_29:09:af (00:e1:6d:29:09:af)
      Antenna ID: 0x00
      Parent Timing Synchronization Function (TSF): 0x00000000
Tag: Vendor Specific: Apple
    Tag Number: Vendor Specific (221)
    Tag length: 24
    OUI: 00-17-f2 (Apple)
```

# Creación Banco de Pruebas

- Detección de Fallos
  - Ping continuo a su dirección IP
  - Salida de consola al dispositivo, si aplica
  - Inspección visual de la pantalla, si aplica
  - Uso de la pantalla
  - Captura de tráfico sobre el aire

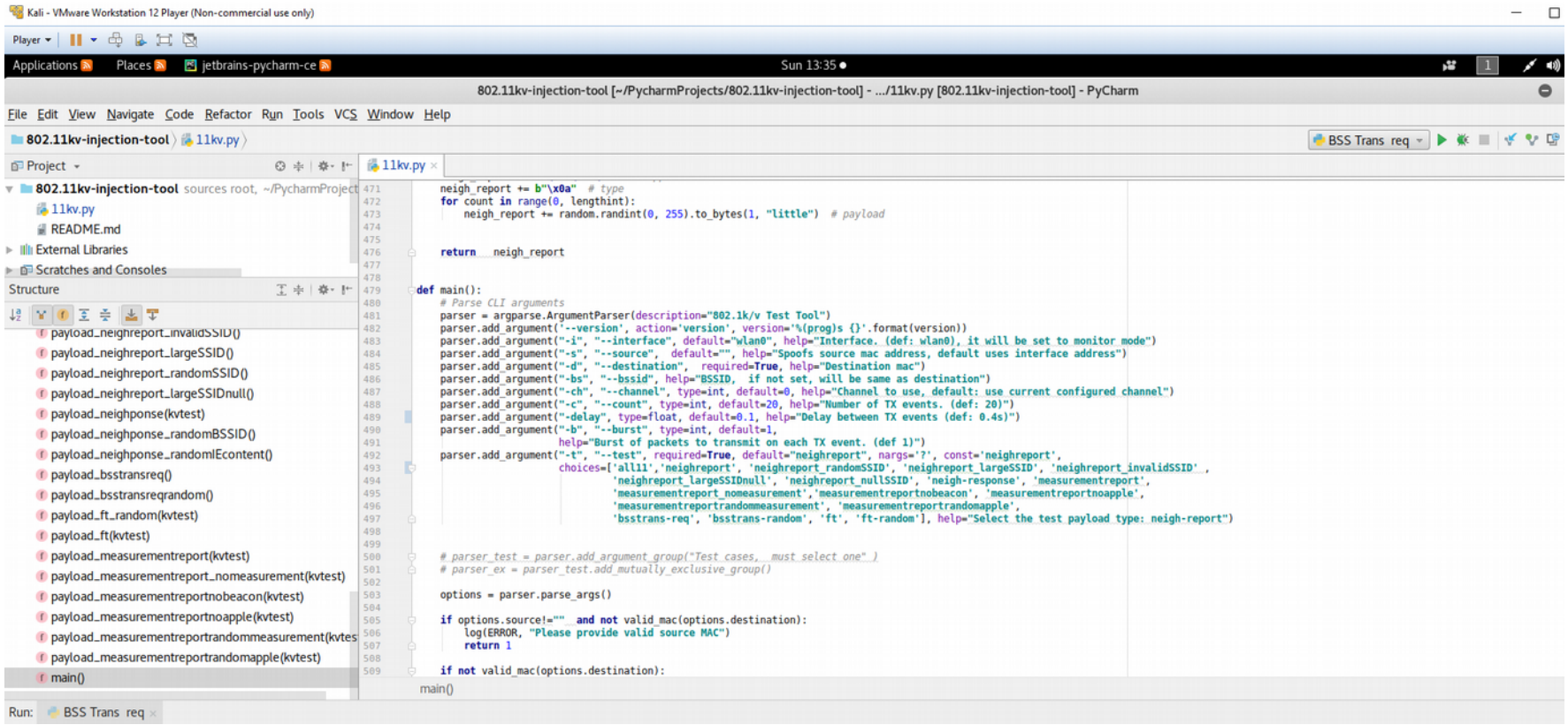
# Creación Banco de Pruebas

| Pruebas | Descripcíon |
|---|---|
| **all11** | Fuerza Bruta sobre todos las categorías posibles |
| **neighreport** | Neighbor Report básico |
| **neighreport_randomSSID** | Neighbor Report. IE de SSID aleatorio |
| **neighreport_largeSSID** | Neighbor Report. IE de SSID con longitud máxima |
| **neighreport_invalidSSID** | Neighbor Report. IE de SSID inválido |
| **neighreport_largeSSIDnull** | Neighbor Report. IE de SSID nulo y longitud máxima |
| **neighreport_nullSSID** | Neighbor Report. IE de SSID nulo |
| **neigh_response** | Respuesta de Neighbor list |
| **measurementreport** | Reporte de Medición de radio |
| **measurementreport_nomeasurement** | Reporte de Medición de radio con contenido incompleto |
| **measurementreport_nobeacon** | Reporte de Medición de radio con alteración al campo de beacon |
| **measurementreport_noapple** | Reporte de Medición de radio con campos de fabricante incompleto |
| **measurementreport_randommeasurement** | Reporte de Medición de radio con contenido aleatorio |
| **Measurementreport_randomapple** | Reporte de Medición de radio con campo de contenido de fabricante aleatorio |
| **bsstrans_req** | Petición de transición (roaming) |
| **bsstrans_random** | Petición de transición con contenido aleatorio |

# Implementación de Herramienta

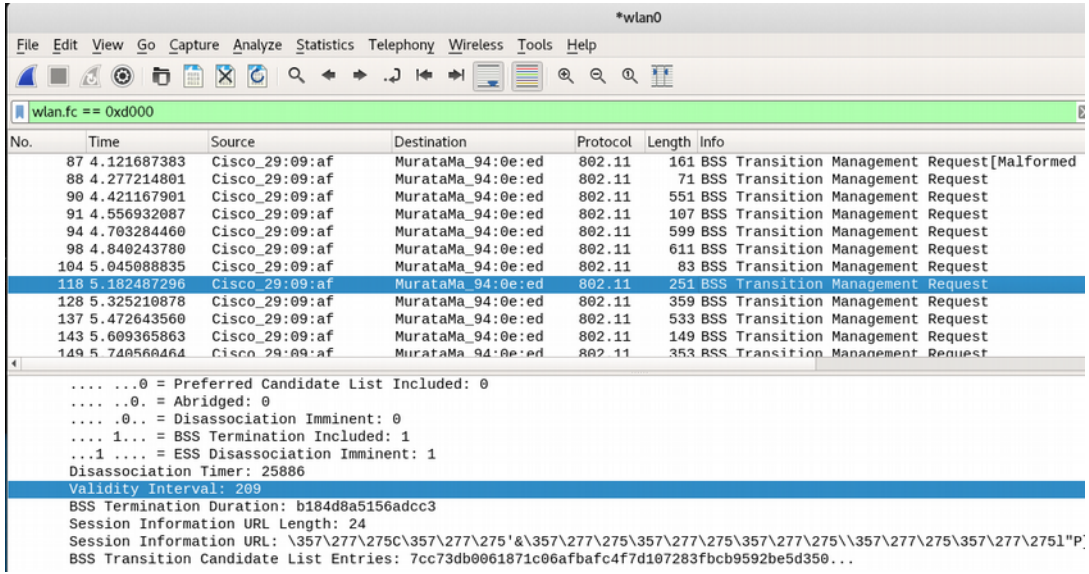
| Comando | Descripcíon |
|---|---|
| **--interface** | Nombre del dispositivo a usar para transmitir |
| **--source** | Dirección origen de la trama |
| **--destination** | Dirección destino de la trama |
| **--bssid** | Dirección a usar para el BSSID |
| **--count** | Cuantas tramas distintas a envíar |
| **--delay** | Retardo entre cada evento de transmisión |
| **--test** | Nombre de la prueba a ejecutar |

# Implementación de Herramienta



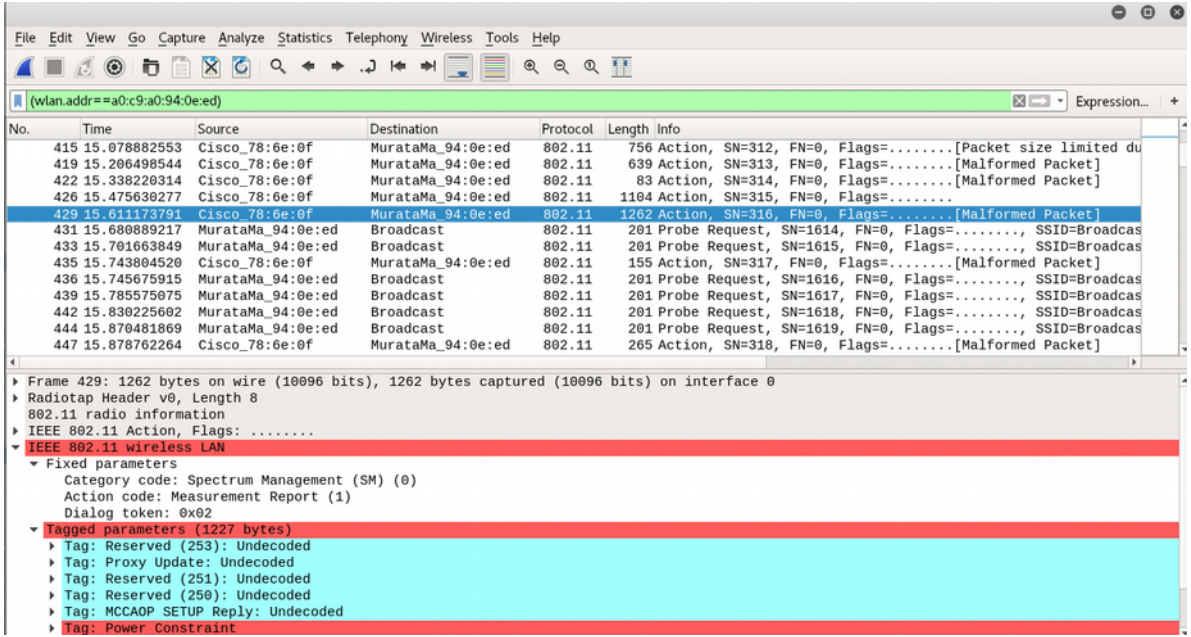
# Resultados

# Resultados




BSS Transition Management Request

# Resultados




Spectrum Management, Measurement Report

# Resultados

- Herramienta disponible
  - Soporte a 14 variaciones/Fuzz testing de diferentes tramas 802.11k/v
  - Soporte a “Brute Force”, todos los tipos, random payload
  - Spoofing de dirección de AP, Cliente, BSSID
  - Repetición de Tramas
  - Burst Mode
- No se encontraron fallos en los clientes
  - Iphone 7
  - Samsung S7/S8
  - iPad Pro

# Conclusiones

- Herramienta sin control de estado
  - Hace Spoofing, pero cliente no espera esa trama
  - Posible codificación errónea de la trama: BSS Transition Request
- Metodología ha funcionado previamente
- Posibles Mejoras
  - Detección de request y envío automático
  - Mejora a las tramas BSS
  - Implementación detallada de cada tipo de trama en los estándares 802.11k/v

# Demo

Gracias!