

Pruebas de Seguridad en implementaciones 802.11k/v

Trabajo Final de Master

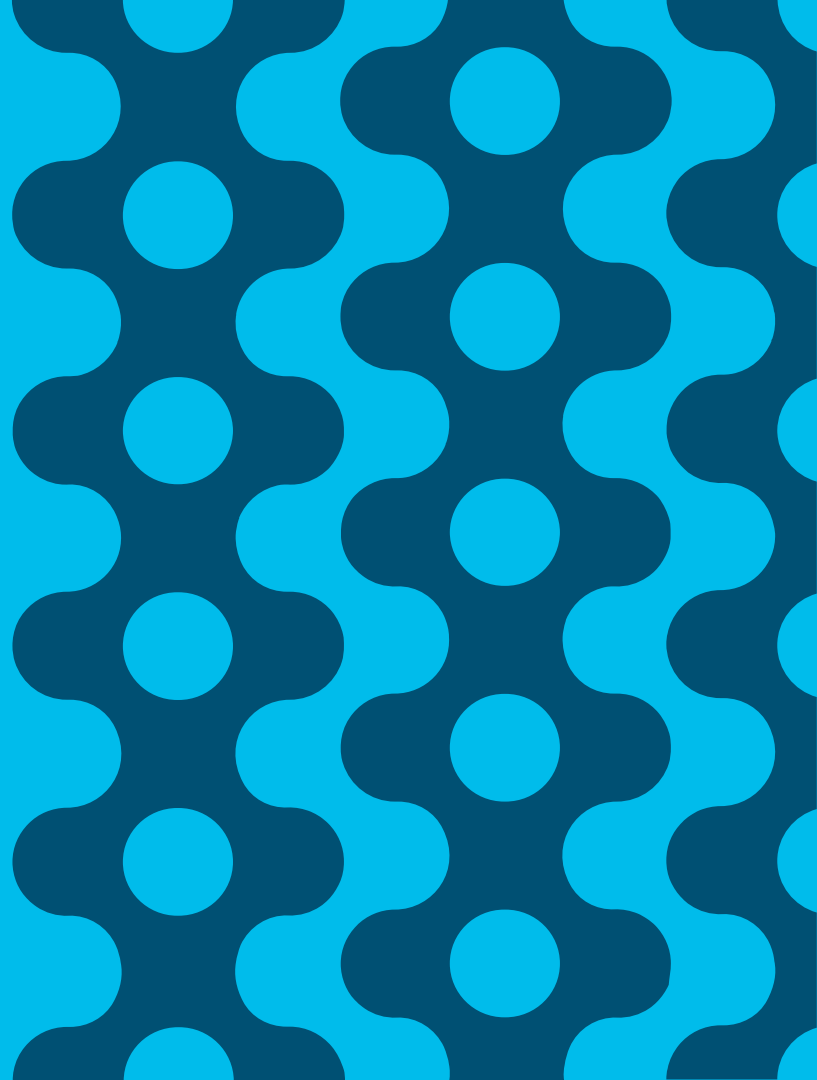
Javier Contreras Albesa
MISTIC - UOC



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, topología, transición
- 802.11r
 - Roaming rápido y seguro entre puntos de acceso

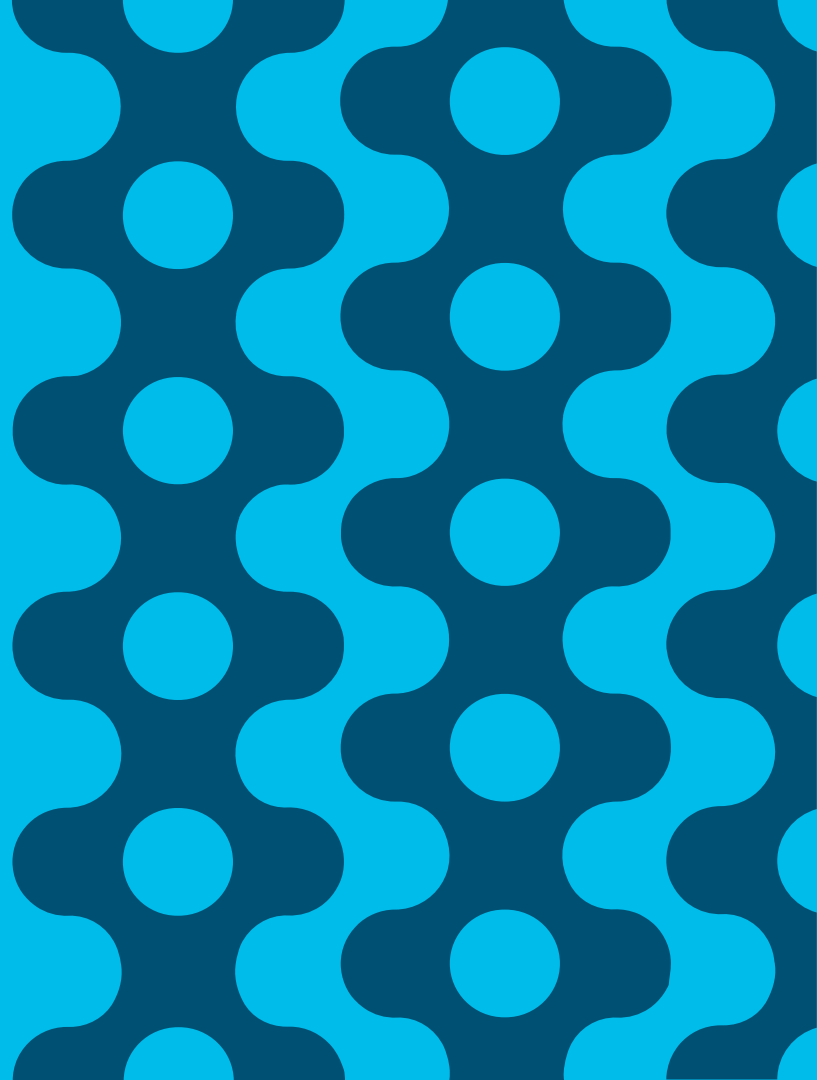


Inicio de una Propuesta

- 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!

Fuzzing

Objetivos



Que hay que hacer?

- Selección de Dispositivos a Evaluar

clients.mikealbano.com

THE LIST HOW TO CONTRIBUTE RANDOMIZER

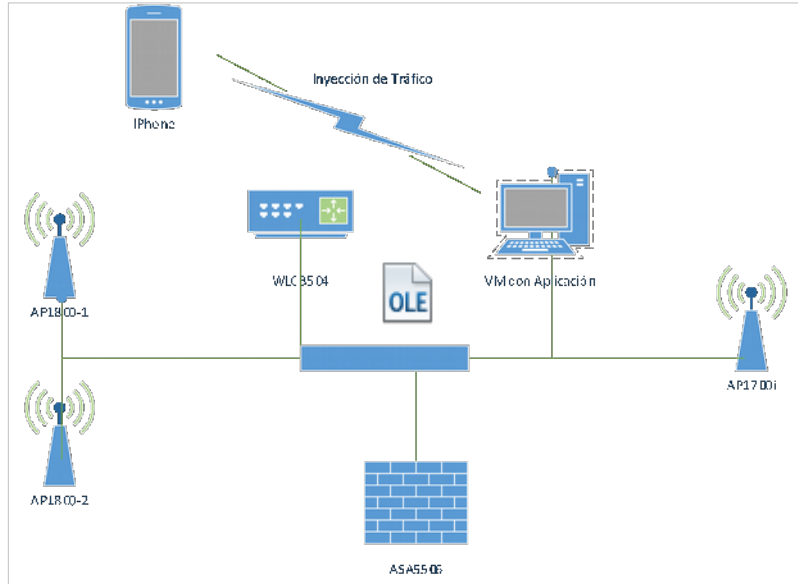
Click a device to download a PCAP of the Association Request frame.

+
 +
 +
 +

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	N	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	N	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
▼ 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)
  ▼ 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)
    .... 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)
▼ Tag: Extended Capabilities (3 octets)
  Tag Number: Extended Capabilities (127)
  Tag length: 3
  > Extended Capabilities: 0x00 (octet 1)
  > Extended Capabilities: 0x00 (octet 2)
  ▼ Extended Capabilities: 0x08 (octet 3)
    .... 0 = TFS: Not supported
    .... 00. = 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
v IEEE 802.11 wireless LAN management frame
  v Fixed parameters
    Category code: Radio Measurement (5)
    Action code: Neighbor Report Request (4)
    Dialog token: 1
  v Tagged parameters (7 bytes)
    v Tag: SSID parameter set: home1
      Tag Number: SSID parameter set (0)
      Tag length: 5
      SSID: home1
```

Petición de Vecinos

Respuesta de Vecinos

```
v IEEE 802.11 wireless LAN management frame
  v Fixed parameters
    Category code: Radio Measurement (5)
    Action code: Neighbor Report Response (5)
    Dialog token: 8
  v Tagged parameters (60 bytes)
    v 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	Descripción
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

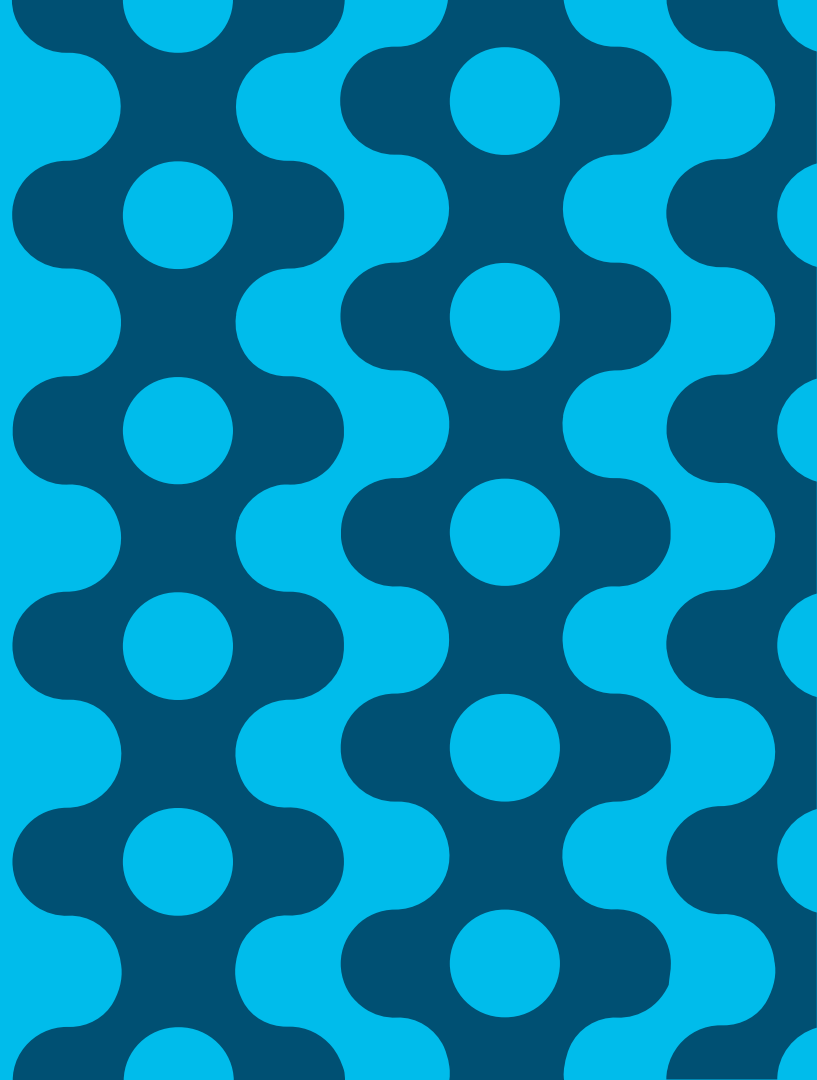
Implementación de Herramienta

Comando	Descripción
--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	Cuántas tramas distintas a enviar
--delay	Retardo entre cada evento de transmisión
--test	Nombre de la prueba a ejecutar

Implementación de Herramienta

```
471     neigh_report += b"\x0a" # type
472     for count in range(0, lengthint):
473         neigh_report += random.randint(0, 255).to_bytes(1, "little") # payload
474
475
476     return __neigh_report
477
478
479 def main():
480     # Parse CLI arguments
481     parser = argparse.ArgumentParser(description="802.1k/v Test Tool")
482     parser.add_argument("--version", action='version', version='%(prog)s {}'.format(version))
483     parser.add_argument("-i", "--interface", default="wlan0", help="Interface. (def: wlan0, it will be set to monitor mode)")
484     parser.add_argument("-s", "--source", default="", help="Spoofs source mac address, default uses interface address")
485     parser.add_argument("-d", "--destination", required=True, help="Destination mac")
486     parser.add_argument("-bs", "--bssid", help="BSSID, if not set, will be same as destination")
487     parser.add_argument("-ch", "--channel", type=int, default=0, help="Channel to use, default: use current configured channel")
488     parser.add_argument("-c", "--count", type=int, default=20, help="Number of TX events. (def: 20)")
489     parser.add_argument("--delay", type=float, default=0.1, help="Delay between TX events (def: 0.4s)")
490     parser.add_argument("-b", "--burst", type=int, default=1,
491                       help="Burst of packets to transmit on each TX event. (def 1)")
492     parser.add_argument("-t", "--test", required=True, default="neighreport", nargs='?', const='neighreport',
493                       choices=['all11', 'neighreport', 'neighreport_randomSSID', 'neighreport_largeSSID', 'neighreport_invalidSSID',
494                                'neighreport_largeSSIDnull', 'neighreport_nullSSID', 'neigh-report', 'measurementreport',
495                                'measurementreport_nomeasurement', 'measurementreport_nobeacon', 'measurementreport_noapple',
496                                'measurementreport_randommeasurement', 'measurementreport_randomapple',
497                                'bsstrans-req', 'bsstrans-random', 'ft', 'ft-random'], help="Select the test payload type: neigh-report")
498
499
500     # parser_test = parser.add_argument_group("Test cases, must select one")
501     # parser_ex = parser_test.add_mutually_exclusive_group()
502
503     options = parser.parse_args()
504
505     if options.source!="" and not valid_mac(options.destination):
506         log(ERROR, "Please provide valid source MAC")
507         return 1
508
509     if not valid_mac(options.destination):
510
511 main()
```


Resultados



Resultados

*wlan0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

wlan.fc == 0xd000

No.	Time	Source	Destination	Protocol	Length	Info
87	4.121687383	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	161	BSS Transition Management Request [Malformed]
88	4.277214801	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	71	BSS Transition Management Request
90	4.421167901	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	551	BSS Transition Management Request
91	4.556932087	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	107	BSS Transition Management Request
94	4.703284460	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	599	BSS Transition Management Request
98	4.840243780	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	611	BSS Transition Management Request
104	5.045088835	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	83	BSS Transition Management Request
118	5.182487296	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	251	BSS Transition Management Request
128	5.325210878	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	359	BSS Transition Management Request
137	5.472643560	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	533	BSS Transition Management Request
143	5.609365863	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	149	BSS Transition Management Request
149	5.740560464	Cisco_29:09:af	MurataMa_94:0e:ed	802.11	353	BSS Transition Management Request

.... ..0 = Preferred Candidate List Included: 0
.... ..0. = Abridged: 0
.... ..0.. = Disassociation Imminent: 0
.... ..1... = BSS Termination Included: 1
.... ..1.... = ESS Disassociation Imminent: 1
Disassociation Timer: 25886
Validity Interval: 209
BSS Termination Duration: b184d8a5156adcc3
Session Information URL Length: 24
Session Information URL: \357\277\275C\357\277\275'&\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275\357\277\275"
BSS Transition Candidate List Entries: 7cc73db0061871c06afbafcf4f7d107283fcb9592be5d350...

BSS Transition Management Request

Resultados

The screenshot shows a Wireshark capture of IEEE 802.11 wireless LAN traffic. The main pane displays a list of frames with the following columns: No., Time, Source, Destination, Protocol, Length, and Info. Frame 429 is highlighted in blue. The details pane for frame 429 is expanded, showing the IEEE 802.11 wireless LAN structure. The 'Fixed parameters' section includes: Category code: Spectrum Management (SM) (0), Action code: Measurement Report (1), and Dialog token: 0x02. The 'Tagged parameters (1227 bytes)' section is expanded, showing several tags: Tag: Reserved (253): Undecoded, Tag: Proxy Update: Undecoded, Tag: Reserved (251): Undecoded, Tag: Reserved (250): Undecoded, Tag: MCCAOP SETUP Reply: Undecoded, and Tag: Power Constraint.

No.	Time	Source	Destination	Protocol	Length	Info
415	15.078882553	Cisco_78:6e:0f	MurataMa_94:0e:ed	802.11	756	Action, SN=312, FN=0, Flags=.....[Packet size limited du
419	15.206498544	Cisco_78:6e:0f	MurataMa_94:0e:ed	802.11	639	Action, SN=313, FN=0, Flags=.....[Malformed Packet]
422	15.338220314	Cisco_78:6e:0f	MurataMa_94:0e:ed	802.11	83	Action, SN=314, FN=0, Flags=.....[Malformed Packet]
426	15.475630277	Cisco_78:6e:0f	MurataMa_94:0e:ed	802.11	1104	Action, SN=315, FN=0, Flags=.....
429	15.611173791	Cisco_78:6e:0f	MurataMa_94:0e:ed	802.11	1262	Action, SN=316, FN=0, Flags=.....[Malformed Packet]
431	15.680899217	MurataMa_94:0e:ed	Broadcast	802.11	201	Probe Request, SN=1614, FN=0, Flags=....., SSID=Broadcas
433	15.701663849	MurataMa_94:0e:ed	Broadcast	802.11	201	Probe Request, SN=1615, FN=0, Flags=....., SSID=Broadcas
435	15.743804520	Cisco_78:6e:0f	MurataMa_94:0e:ed	802.11	155	Action, SN=317, FN=0, Flags=.....[Malformed Packet]
436	15.745675915	MurataMa_94:0e:ed	Broadcast	802.11	201	Probe Request, SN=1616, FN=0, Flags=....., SSID=Broadcas
439	15.785575075	MurataMa_94:0e:ed	Broadcast	802.11	201	Probe Request, SN=1617, FN=0, Flags=....., SSID=Broadcas
442	15.830225602	MurataMa_94:0e:ed	Broadcast	802.11	201	Probe Request, SN=1618, FN=0, Flags=....., SSID=Broadcas
444	15.870481869	MurataMa_94:0e:ed	Broadcast	802.11	201	Probe Request, SN=1619, FN=0, Flags=....., SSID=Broadcas
447	15.878762264	Cisco_78:6e:0f	MurataMa_94:0e:ed	802.11	265	Action, SN=318, FN=0, Flags=.....[Malformed Packet]

Frame 429: 1262 bytes on wire (10096 bits), 1262 bytes captured (10096 bits) on interface 0

- Radiotap Header v0, Length 8
- 802.11 radio information
- IEEE 802.11 Action, Flags:
- IEEE 802.11 wireless LAN**
 - Fixed parameters
 - Category code: Spectrum Management (SM) (0)
 - Action code: Measurement Report (1)
 - Dialog token: 0x02
 - Tagged parameters (1227 bytes)**
 - Tag: Reserved (253): Undecoded
 - Tag: Proxy Update: Undecoded
 - Tag: Reserved (251): Undecoded
 - Tag: Reserved (250): Undecoded
 - Tag: MCCAOP SETUP Reply: Undecoded
 - Tag: Power Constraint

Spectrum Management, Measurement Report

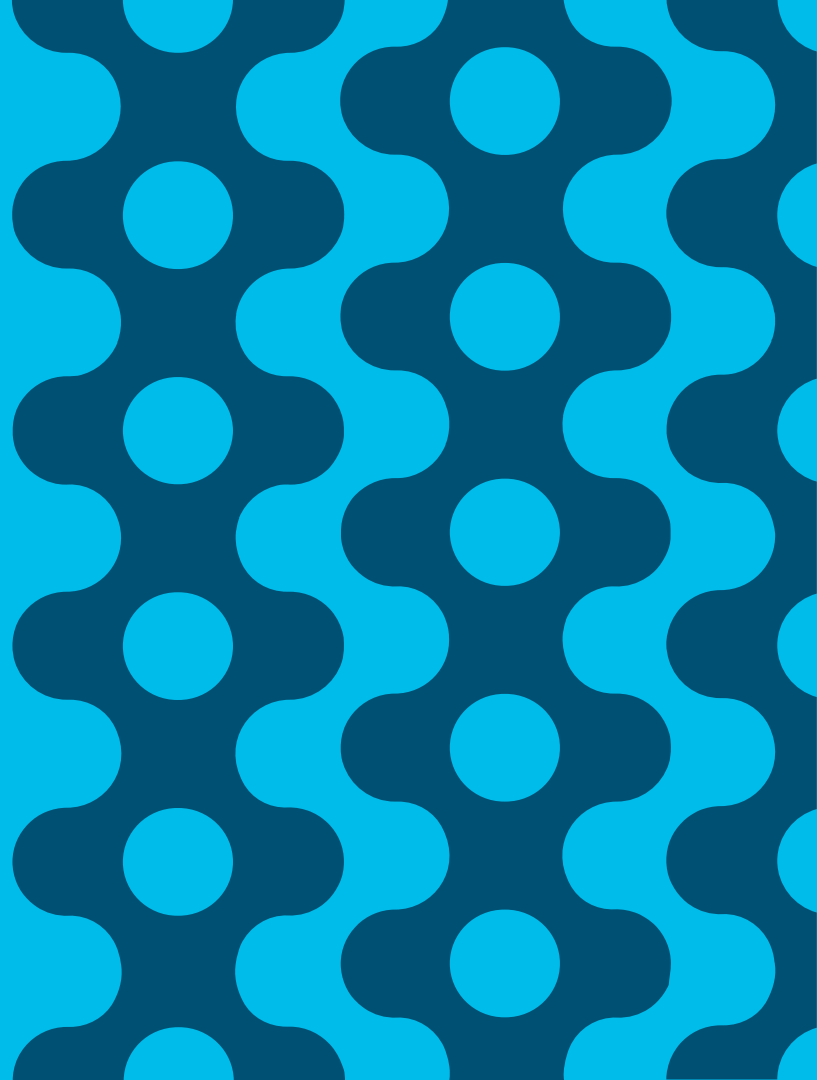
Resultados

- 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!

