Advanced Mutation Fuzzing Method For Wireless Protocols

Lidong LI & Xianzi Kong

Catarc@Intelligent Connected Vehicle Cyber Security AD-LAB

数据资源中心
Automotive Data Center

About us

Lidong LI:

Communication Protocol Security Research Team Leader
Bug Hunter
Wireless(802.11&Bluetooth&BLE) Protocol Security Research
Fuzzing

Xianzi Kong:

Security engineer
CTFer
Crypto Research
Protocol Security Research

数据资源中心
Automotive Data Center

Agenda

- protocol stack analysis
- Attack vulnerable drivers
- Advanced Mutation Fuzzing
- Conclusion

数据资源中心
Automotive Data Center

About Wireless Fuzzing ?

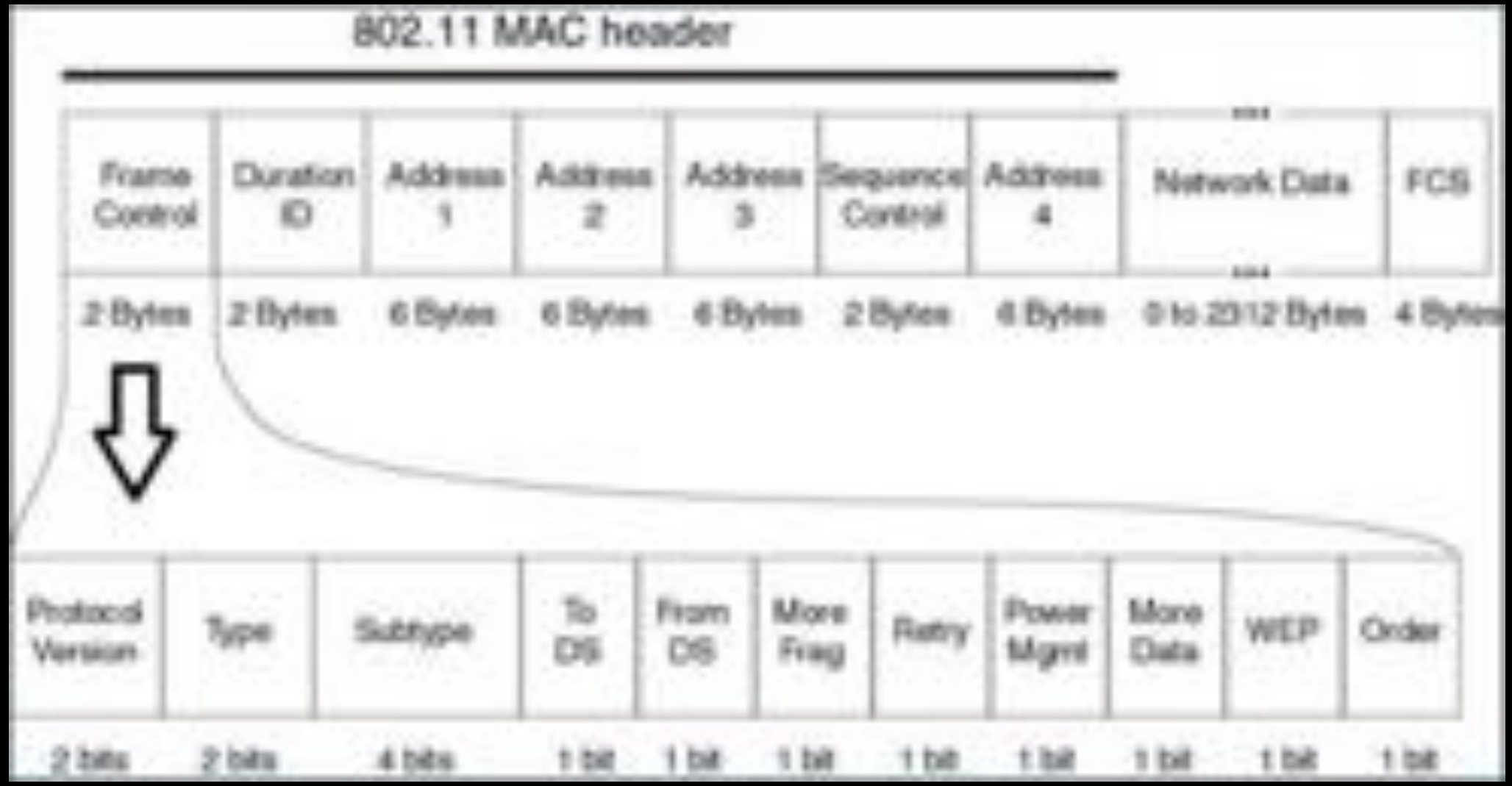
- After the target receives the malformed data……
- Our target is **Phone , Wireless** adapter , Smart Devices , IOT Devices…
- All wifi connected smart devices
- **OverFlow** ? **Crash** ? **Denial of service** ?
- Car wireless module
- Wireless frame in the air SO….
- Exploit….**RCE** ! ! ! !

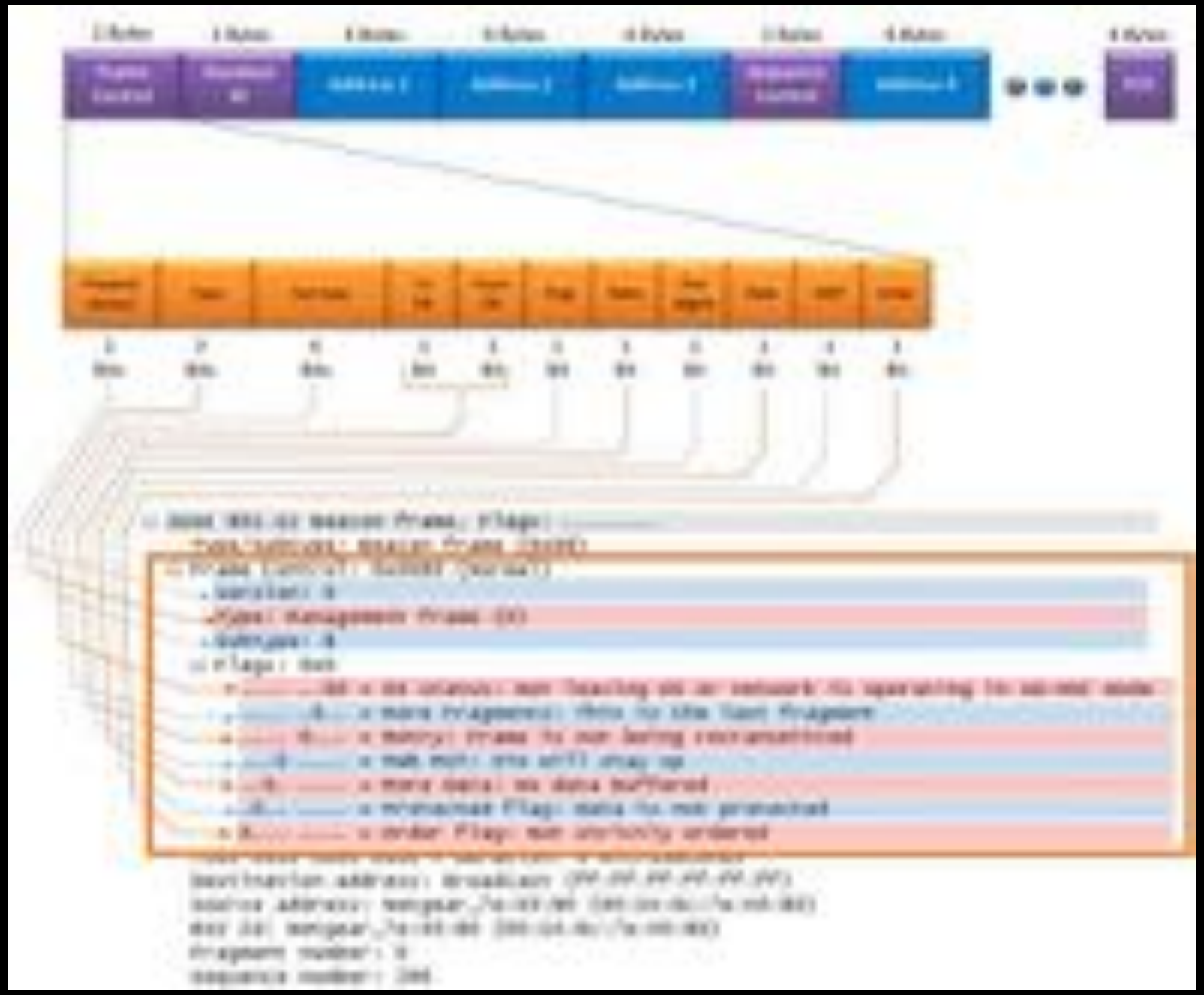
数据资源中心
Automotive Data Center

protocol stack analysis

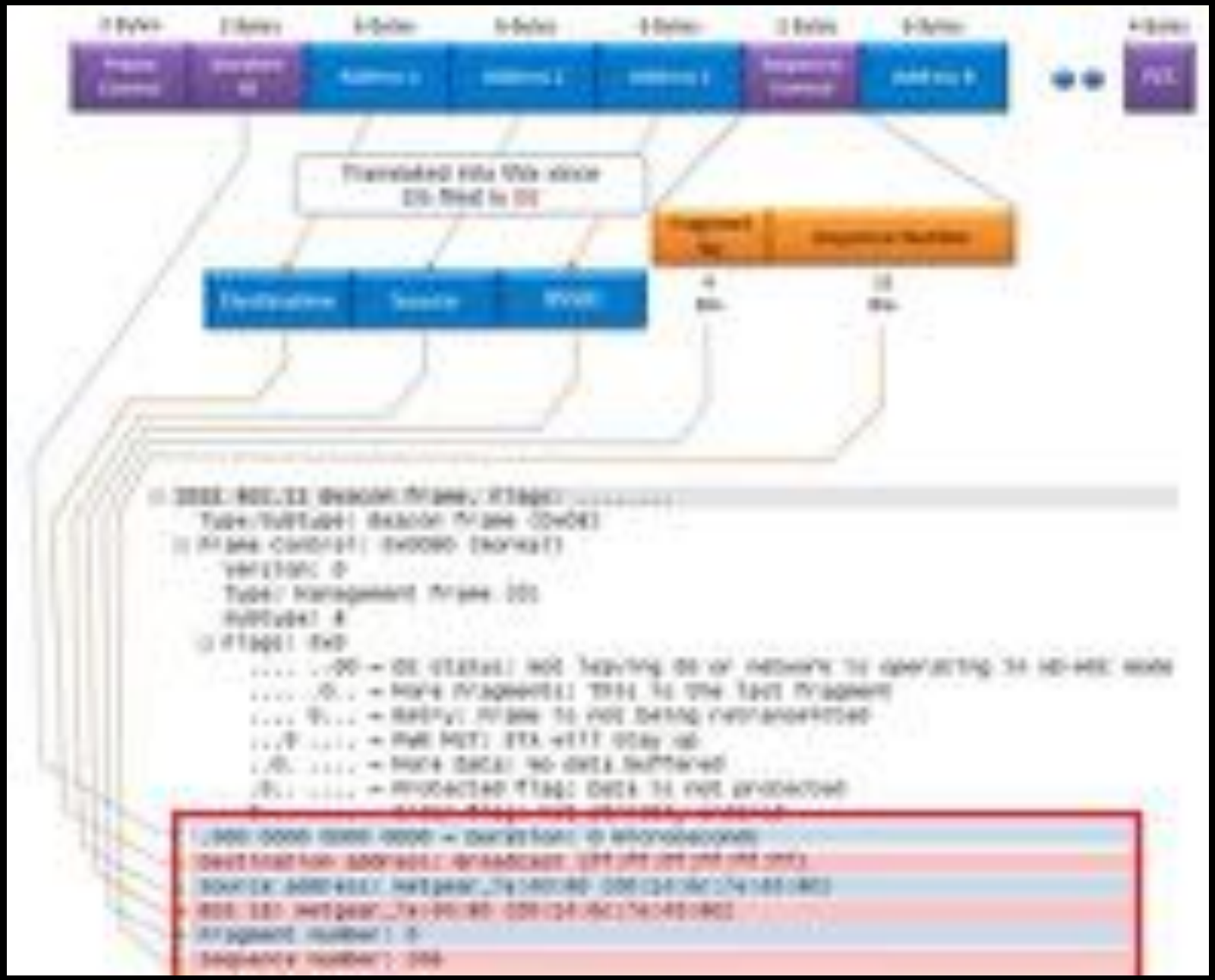
数据资源中心
Automotive Data Center

protocol stack analysis





数据资源中心
Automotive Data Center



数据资源中心
Automotive Data Center

Attack vulnerable drivers

数据资源中心
Automotive Data Center

Classic fuzzing

example:

```
brcmf_cfg80211_start_ap(   struct cfg80211_ap_settings *settings ) {
        s32  ie_offset;
        struct brcmf_tlv *ssid_ie;
        struct brcmf_ssid_le ssid_le;

        memset( &ssid_le, 0, sizeof(ssid_le) );

        if  ( settings->ssid == NULL || settings->ssid_len == 0 ) {
                ie_offset = DOT11_MGMT_HDR_LEN +
DOT11_BCN_PRB_FIXED_LEN;
                ssid_ie = brcmf_parse_tlvs( (u8
*)&settings->beacon.head[ie_offset], settings->beacon.head_len -
ie_offset, WLAN_EID_SSID );
                if ( !ssid_ie )
                        return -EINVAL;

                memcpy( ssid_le.SSID, ssid_ie->data,
ssid_ie->len );   //overflow here.
                ssid_le.SSID_len = cpu_to_le32( ssid_ie->len );
        }
        else {
                memcpy( ssid_le.SSID, settings->ssid,
settings->ssid_len );
                ssid_le.SSID_len = cput_to_le32( (u32)settings->ssid_len);
        }
        ...
    });
        }
```

数据资源中心
Automotive Data Center

Fuzzing testing example

- Management frame tag other than SSID?
- Supported Rates….
- Channel…
- EXRates…
- Traffic Indication Map (TIM)

```
▸Frame 12: 322 bytes on wire (2576 bits), 322 bytes captured (2576 bits) on
▸Radiotap Header v0, Length 18
▸802.11 radio information
▸IEEE 802.11 Beacon frame, Flags: ........
▾IEEE 802.11 wireless LAN
  Fixed parameters (12 bytes)
  ▾Tagged parameters (268 bytes)
    ▸Tag: SSID parameter set: DIRECT-xZSAKURAKHCRmsLW
    ▸Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    ▸Tag: DS Parameter set: Current Channel: 8
    ▸Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
```

数据资源中心
Automotive Data Center

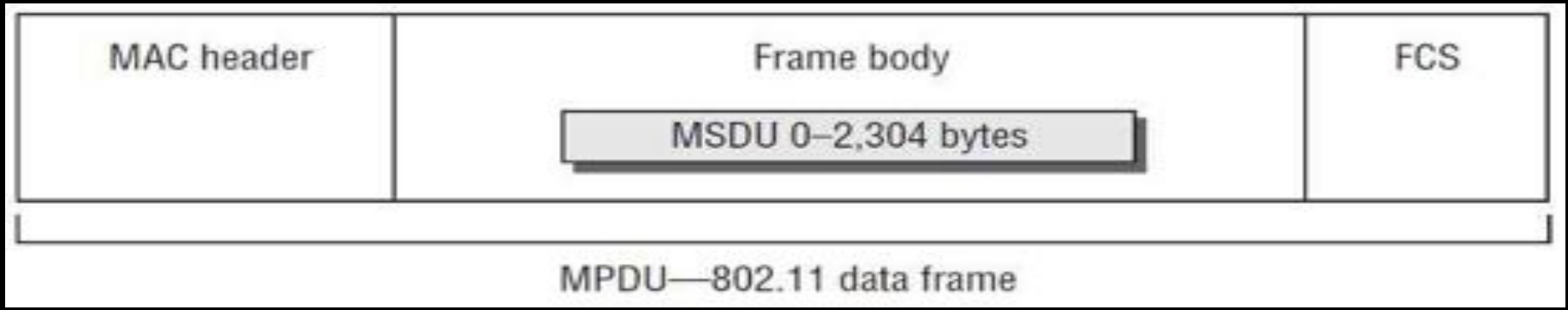
Different types of frame bodies contain different information elements.

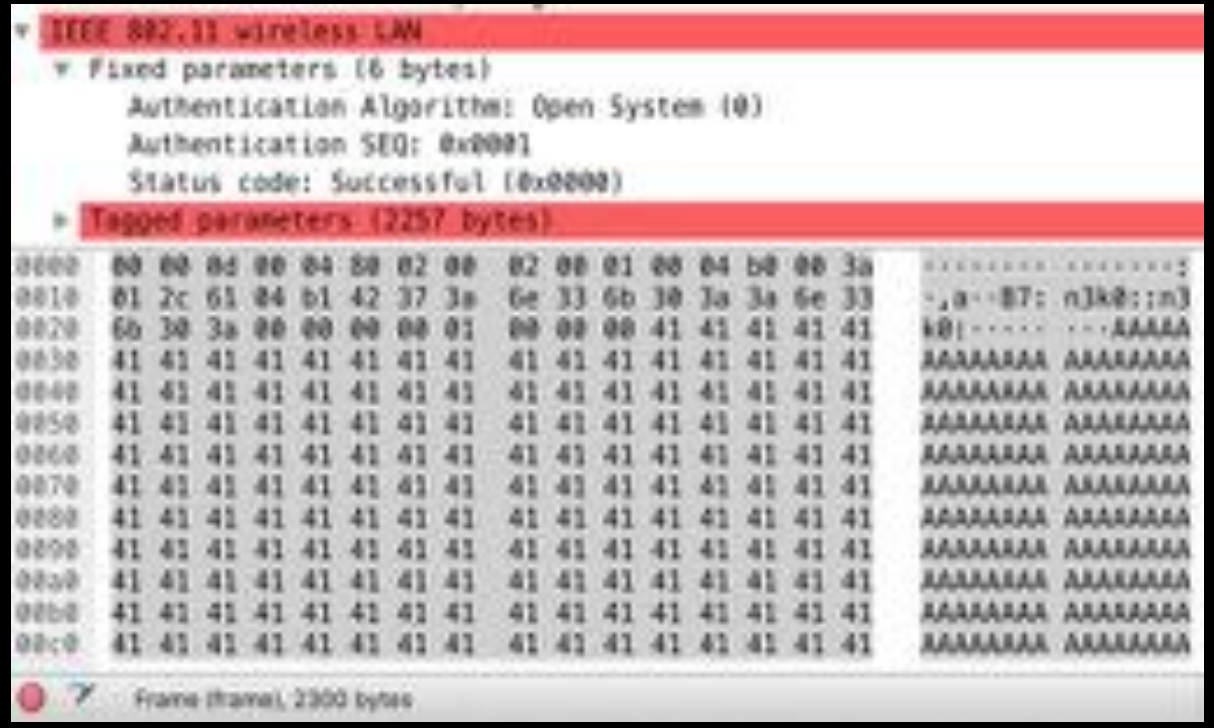
- 802.11 protocol certain the minimum and maximum length of each element-certain information field.

- **Long or short IE length in fuzzing testing.**

- **Each type of frame contains its own** certain **information elements.**

数据资源中心
Automotive Data Center





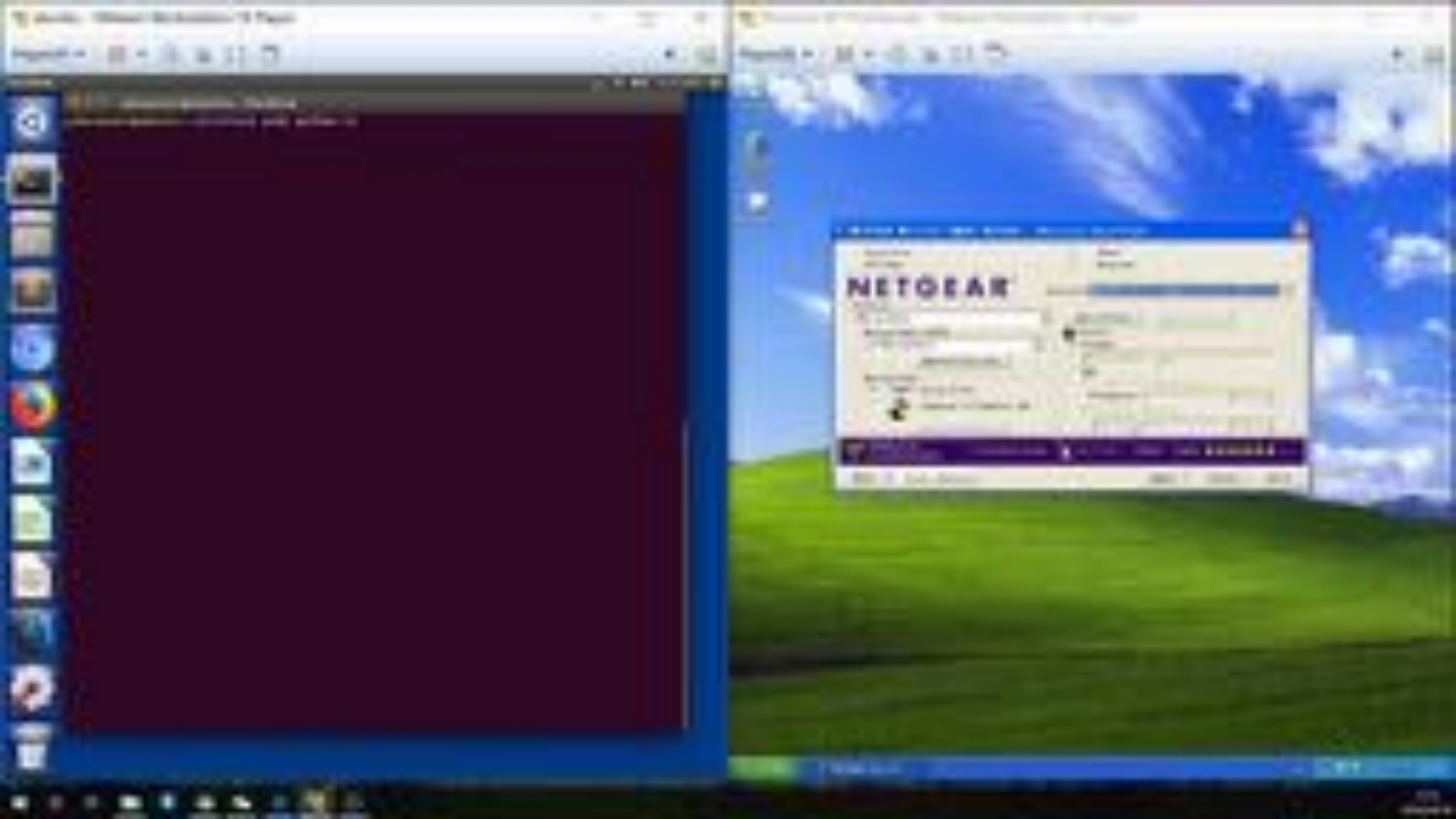
- **The maximum 802.11 MTU is 2304 bytes!!!**

MTU + MAC Header + Encryption Header

- **WEP : 2304 + 34 + 8 = 2346 bytes**
- **WPA (TKIP) : 2304 + 34 + 20 = 2358 bytes**
- **WPA2 (CCMP) : 2304 + 34 + 16 = 2354 bytes**

数据资源中心
Automotive Data Center

Demo


NETGEAR

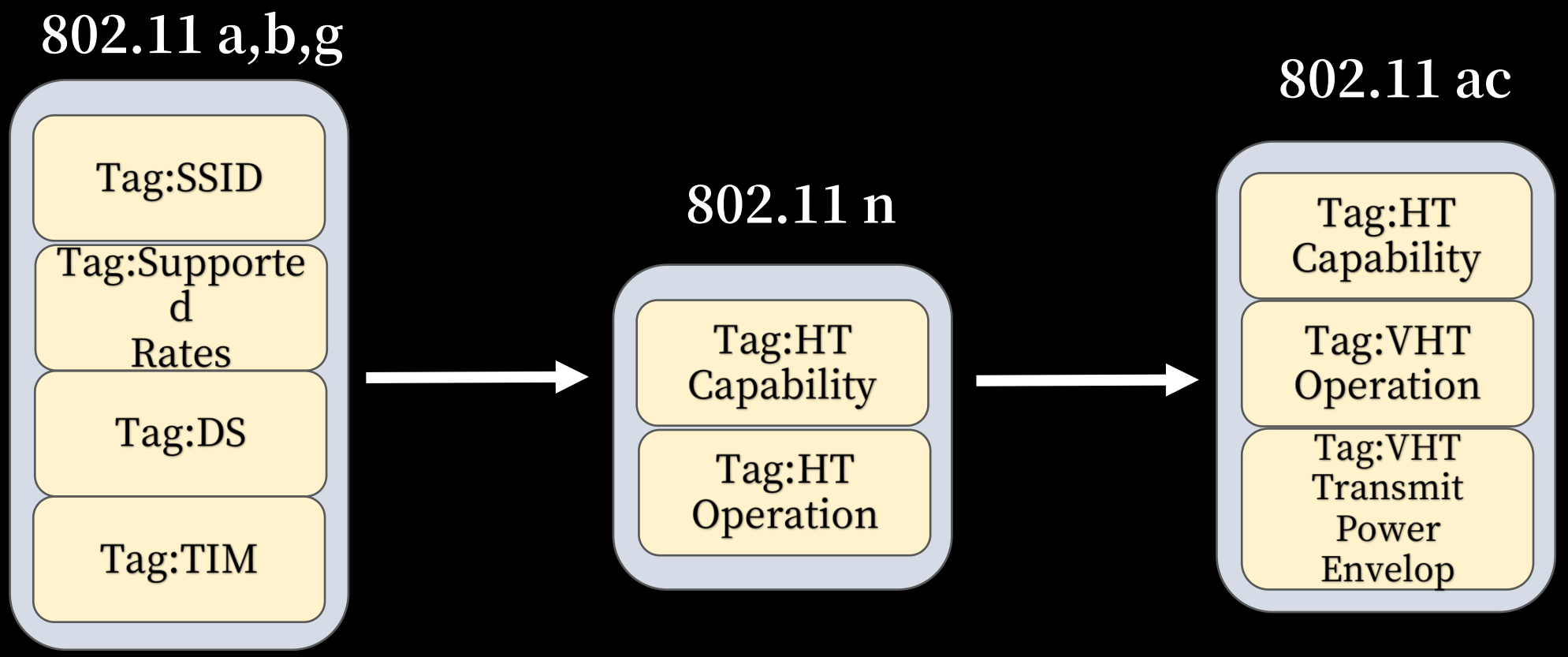
Advanced Mutation Fuzzing

数据资源中心
Automotive Data Center

How to design a smart mutation strategy? ?

Frequency range / Type	PHY	Protocol	Release date[1]	Frequency	Bandwidth	Stream data rate[1]	Kilometer (MIMO streams)	Modulation	Approximate range[Indoor/outdoor assumed]	
				(GHz)	(MHz)	(Mbit/s)			Indoor	Outdoor
1-6GHz	[illegible]	802.11-1997	Jun 1997	2.4	22	1, 2	n/a	[illegible], FHSS	20 m (66 ft)	100 m (330 ft)
	HR [illegible][2]	802.11b	Sep 1999	2.4	22	1, 2, 5.5, 11	n/a	[illegible]	35 m (115 ft)	140 m (460 ft)
	OFDM	802.11a	Sep 1999	5	[illegible]	6, 9, 12, 18, 24, 36, 48, 54 (for 20MHz bandwidth, divide by 2 and 4 for 10 and 5 MHz)	n/a	OFDM	35 m (115 ft)	120 m (390 ft)
		802.11j	Nov 2002	4.9/5.0[3][4][5]					-	-
		802.11p	Jul 2010	5.9					-	1,000 m (3,300 ft)[6][7]
		802.11n	Nov 2009	2.4/5[8]					-	5,000 m (16,500 ft)[8]
	DSSS-CHSM, etc.)	802.11g	Jun 2003	2.4					38 m (125 ft)	140 m (460 ft)
	HT-OFDM[9]	802.11n	Oct 2009	2.4/5	20	Up to 288.8[10]	4	MIMO-OFDM	70 m (230 ft)	250 m (820 ft)[10]
					40	Up to 600[10]				
	VHT-OFDM[11]	802.11ac	Dec 2013	5	20	Up to 346.8[10]	8	MIMO-OFDM	35 m (115 ft)[12]	-
					40	Up to 800[10]				
					80	Up to 1733.2[10]				
					160	Up to 3466.8[10]				

数据资源中心
Automotive Data Center

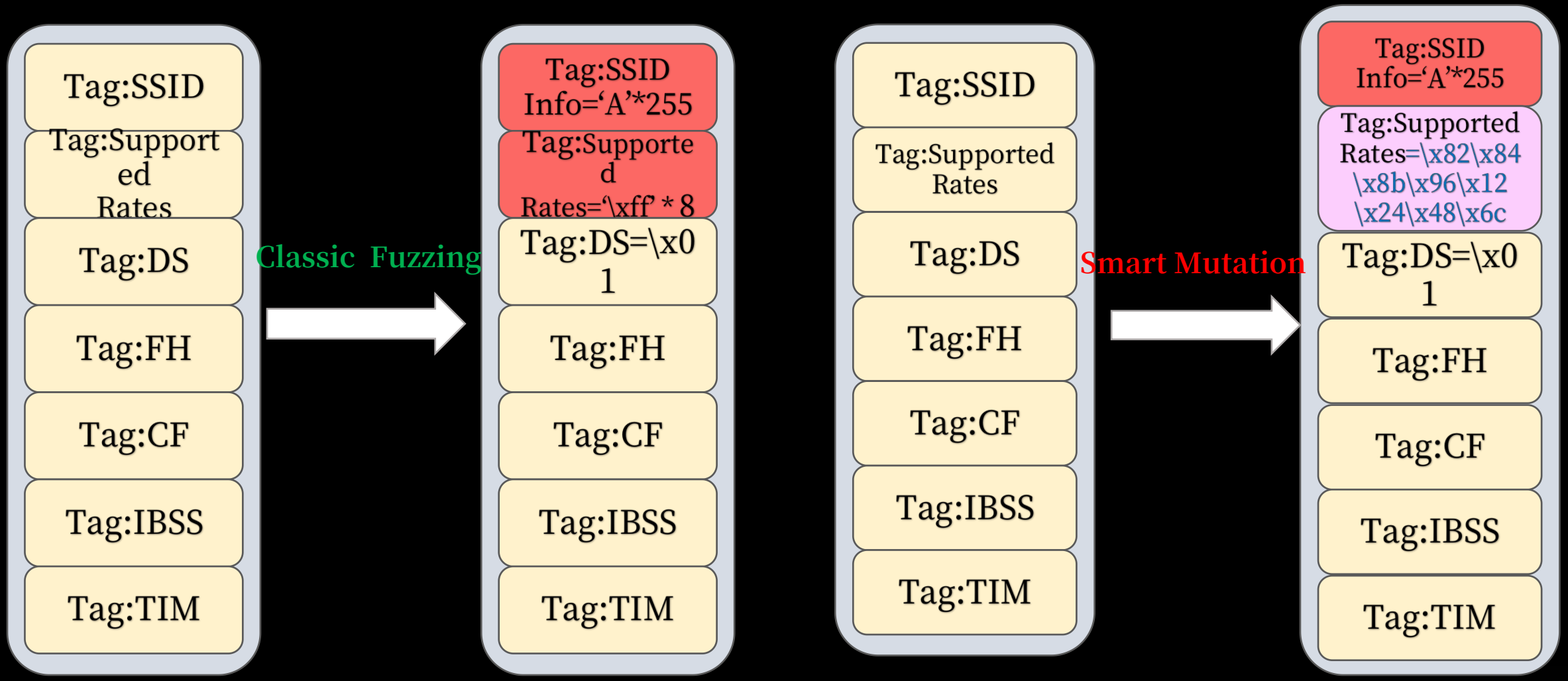


数据资源中心
Automotive Data Center

Core specification

```
▾IEEE 802.11 wireless LAN
  ▸Fixed parameters (4 bytes)
  ▾Tagged parameters (15 bytes)
    ▸Tag: SSID parameter set: AAA
    ▾Tag: Supported Rates BSS requires support for mandatory features of HT PHY (IEEE 802.11 - Clause 20), BSS r
      Tag Number: Supported Rates (1)
      Tag length: 8
      Supported Rates: BSS requires support for mandatory features of HT PHY (IEEE 802.11 - Clause 20) (0xff)
      Supported Rates: BSS requires support for mandatory features of HT PHY (IEEE 802.11 - Clause 20) (0xff)
      Supported Rates: BSS requires support for mandatory features of HT PHY (IEEE 802.11 - Clause 20) (0xff)
      Supported Rates: BSS requires support for mandatory features of HT PHY (IEEE 802.11 - Clause 20) (0xff)
      Supported Rates: BSS requires support for mandatory features of HT PHY (IEEE 802.11 - Clause 20) (0xff)
      Supported Rates: BSS requires support for mandatory features of HT PHY (IEEE 802.11 - Clause 20) (0xff)
      Supported Rates: BSS requires support for mandatory features of HT PHY (IEEE 802.11 - Clause 20) (0xff)
      Supported Rates: BSS requires support for mandatory features of HT PHY (IEEE 802.11 - Clause 20) (0xff)
```

数据资源中心
Automotive Data Center



数据资源中心
Automotive Data Center

Beacon

- Tag:SSID
- Tag:Supported Rates
- Tag:Extended Rates
- Tag:Vendor Specific
- Tag:TIM

→

ProbeResp

- Tag:SSID
- Tag:Supported Rates
- Tag:Extended Rates
- Tag:Vendor Specific
- Tag:TIM

数据资源中心
Automotive Data Center

Detail mutation for Frame Tag subtype ?

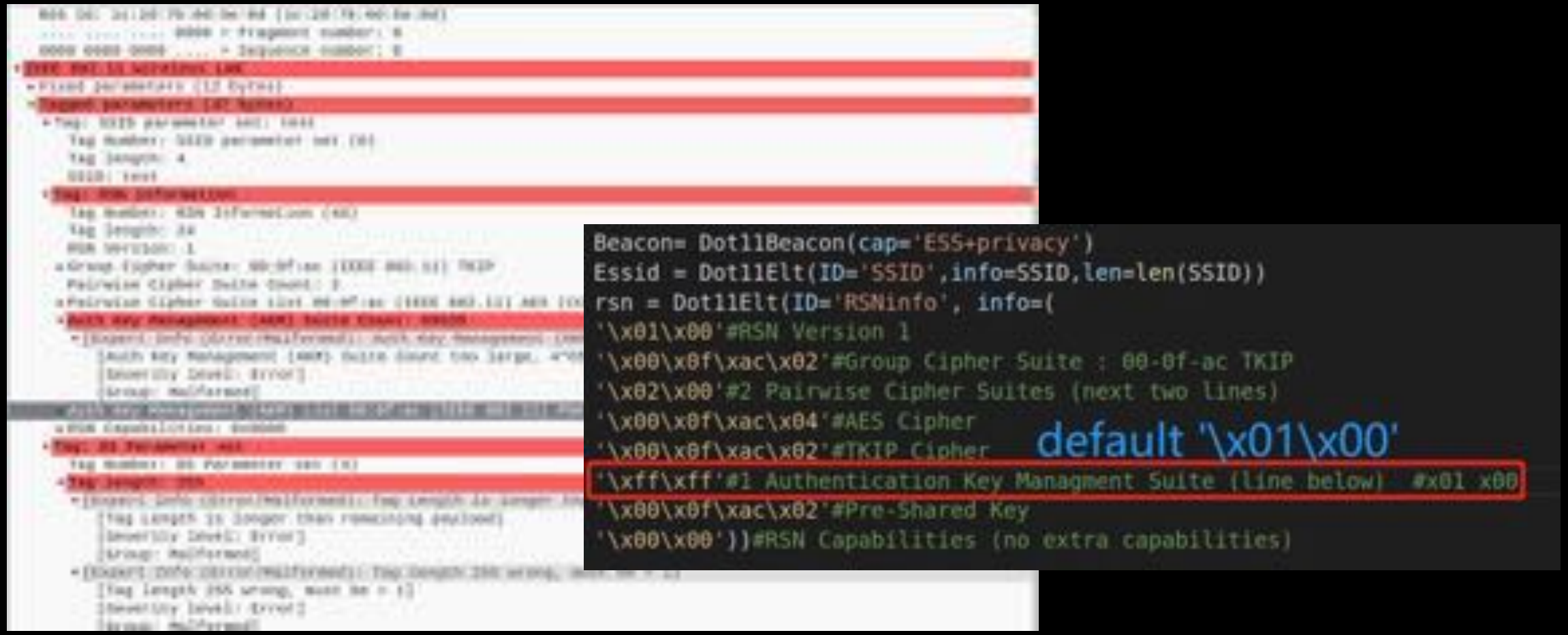
The RSN Information Element is provided below. The Size of the RSN IE is limited to a maximum of 255 bytes

	Element ID	length	Version	Group Data Cipher Suite	Pairwise Cipher Suite Count	Pairwise Cipher Suite List
Octets	1	1	2	4	2	4 * **m**

	AKM Suite Count	AKM Suite List	RSN Capabilities	PMKIDCount	PMKID List	Group Management Cipher Suite
Octets	2	4*n	2	2	16*s	4

数据资源中心
Automotive Data Center

Broadcom BCM4325、BCM4329 Denial of service



数据资源中心
Automotive Data Center

OUI	Suite Type	Meaning
00-0F-AC	0	Use group Cipher suite
00-0F-AC	2	TKIP
…	…	…

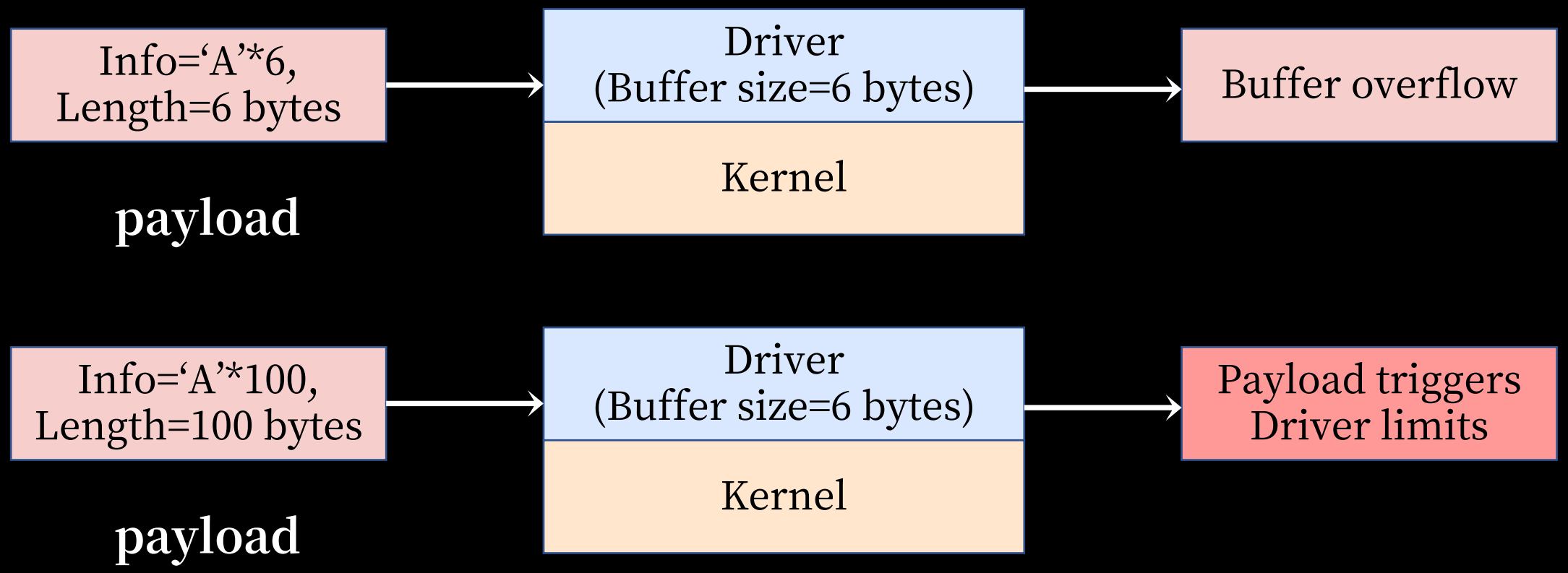
standard protocol format

OUI	Suite Type	Meaning
00-00-00	Number (Non-protocol restricted content)	unknown
FF-FF-FF		
…		

non-standard protocol format

OUI	Suite Type	Meaning
AAAAAAAAAAAA…	Number (Protocol restricted content)	unknown
\u0041\u0041\u0031…		
AA&#65…		
…		

数据资源中心
Automotive Data Center



数据资源中心
Automotive Data Center

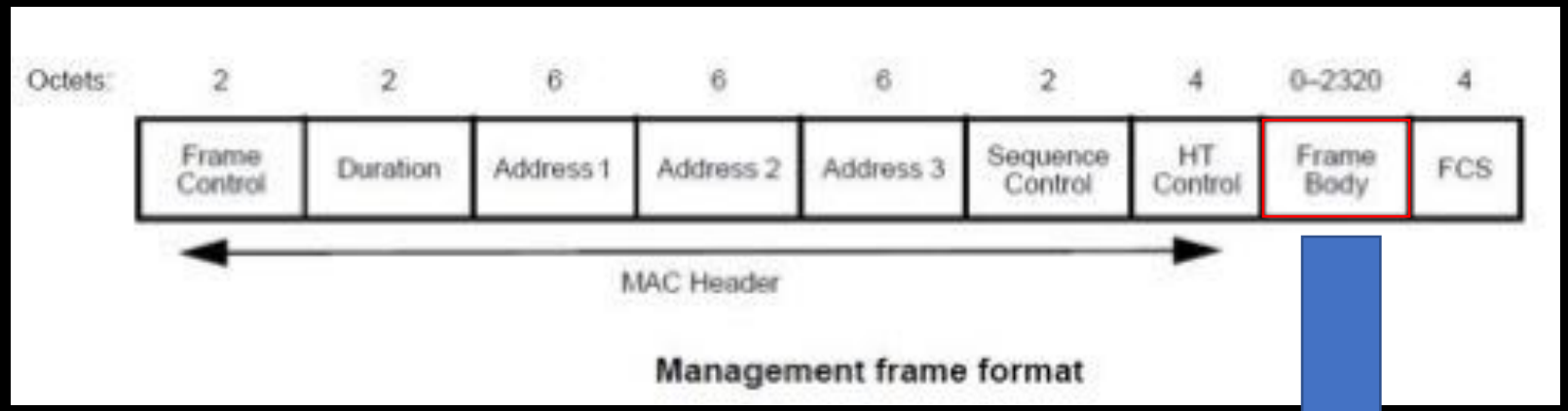
```
RSN = Dot11EltRSN(version=1,
                  group_cipher_suite=RSNCipherSuite(oui=0x0fac,cipher=0x04),#
                  se_cipher_suites=50,
                  cipher_suites=[
                  pherSuite(oui=0x0fac,cipher=RandNum(0,0xff))
                  i in range(50)
```

```
▾ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) Unknown 108 00:0f:ac
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) Unknown 108
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: Unknown (108)
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) Unknown 30
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: Unknown (30)
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) Unknown 66
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: Unknown (66)
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) Unknown 178
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: Unknown (178)
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) Unknown 69
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: Unknown (69)
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) Unknown 17
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: Unknown (17)
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) Unknown 242
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: Unknown (242)
  ▾ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) Unknown 38
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: Unknown (38)
```

```
▾ IEEE 802.11 wireless LAN
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (278 bytes)
    ▸ Tag: Supported Rates 1(B), 2(B), 5.5(B), 11(B), 9, 18, 36, 54, [Mbit/sec]
    ▸ Tag: DS Parameter set: Current Channel: 11
    ▸ Tag: ERP Information
    ▸ Tag: SSID parameter set: n3k0
    ▾ Tag: RSN Information
        Tag Number: RSN Information (48)
        Tag length: 252
        RSN Version: 1
      ▸ Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      ▾ Pairwise Cipher Suite Count: 100
        ▾ [Expert Info (Error/Malformed): Pairwise Cipher Suite Count too large, 4*100 > 244]
            [Pairwise Cipher Suite Count too large, 4*100 > 244]
            [Severity level: Error]
            [Group: Malformed]
      ▾ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) Unknown 79 00:0f:ac (Ieee 802.11) U
        ▸ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) Unknown 79
```

Detail mutation

数据资源中心
Automotive Data Center



Management frame format

```
00 00 0c 00 04 80 00 00  02 00 10 00 40 00 00 00   ........ ....@...
02 1a 11 f2 2a 6b a0 ab  1b cc 75 00 02 1a 11 f2   ....*k.. ..u.....
2a 6b 00 00 00 32 27 20  55 4e 49 4f 4e 20 53 45   *k...2'  UNION SE
4c 45 43 54 20 31 2c 4c  4f 41 44 5f 46 49 4c 45   LECT 1,L OAD_FILE
28 27 2f 65 74 63 2f 70  61 73 73 77 64 27 29 2c   ('/etc/p asswd'),
31 2c 31 2c 31 3b 2d 2d  01 08 82 84 8b 96 24 30   1,1,1;-- ......$0
48 6c 03 01 06 32 04 0c  12 18 60                  Hl...2.. ..`
```

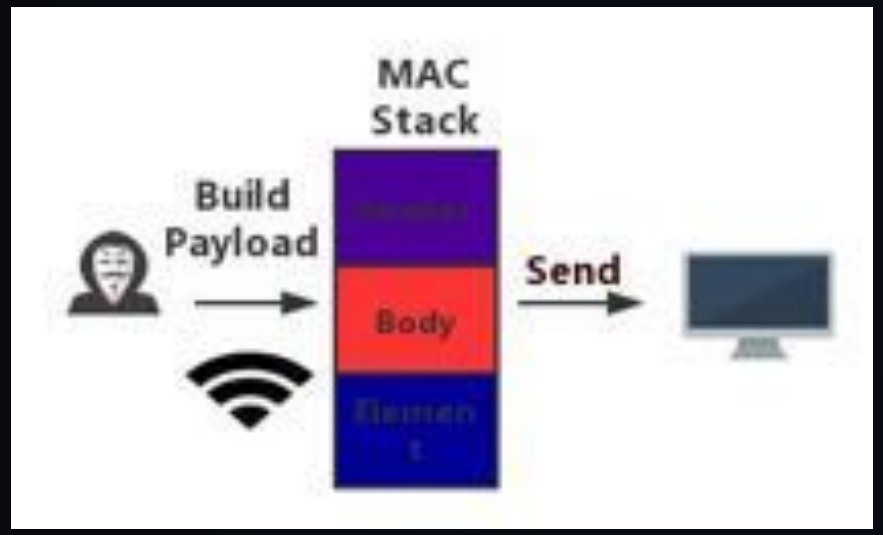
数据资源中心
Automotive Data Center

CVE-2019-12785

CPU 2 U
SLAB: Unable to allocate memory on node 0 (gfp=0x20)

cache: skbuff_head_cache, object size: 256, order: 0

CPU 2 Unable to handle kernel paging request at virtual address 013a00b0, epc == 81615270, ra == 81615258nable to handle kernel paging request at virtual address 013a00b0, epc == 81615270, ra == 81615258



Demo

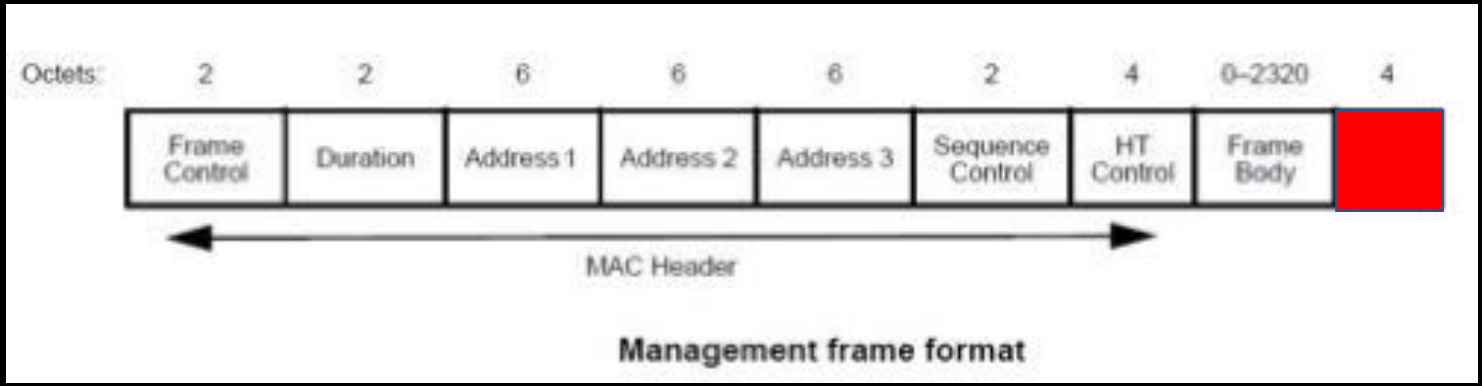
Frame check sequence

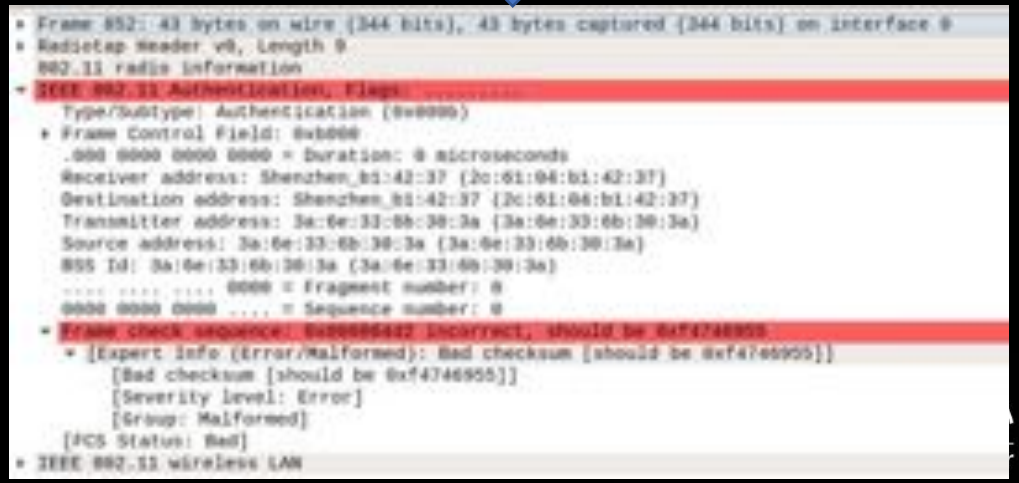
```
Fcs=binascii.crc32(bytes(data)) & 0xFFFFFFFFL
Fcs=hex(fcs)[2:].rstrip('L').decode('hex')[::-1]
```

```
.... .... .... 0000 = Fragment number: 0
0000 0000 0000 .... = Sequence number: 0
Frame check sequence: 0xf4746955 [correct]
[FCS Status: Good]
```

FCS status good------>OK

FCS status Bad------>Error





EAPOL-Type Mutation

```
9   #ifndef CONFIG_H
10  #define CONFIG_H
11
12  #define DEFAULT_EAPOL_VERSION 1
```

Default Version Value

```
66      bss->ap_max_inactivity = AP_MAX_INACTIVITY;
67      bss->eapol_version = EAPOL_VERSION;
68
69      bss->max_listen_interval = 65535;
```

Max Length Value

```
▸Frame 51: 46 bytes on wire (368 bits), 46 bytes captured (36
▸Radiotap Header v0, Length 8
 802.11 radio information
▸IEEE 802.11 QoS Data, Flags: .......T
▸Logical-Link Control
▾802.1X Authentication
  Version: Unknown (173)
  Type: MKA (5)
  Length: 57512
 MACsec Key Agreement
▸[Malformed Packet: EAPOL-MKA]
```

```
802… Probe Request, SN=2064, FN=0, Flags=........, SSID=AD-LAB
802… Probe Response, SN=3852, FN=0, Flags=........, BI=100, SSID=…
802… Probe Response, SN=3853, FN=0, Flags=........, BI=100, SSID=…
802… Authentication, SN=2065, FN=0, Flags=........
802… Probe Response, SN=3854, FN=0, Flags=........, BI=100, SSID=…
802… Authentication, SN=3855, FN=0, Flags=........
802… Association Request, SN=2066, FN=0, Flags=........, SSID=AD-…
802… Association Response, SN=3856, FN=0, Flags=........
EAP… Key (Message 1 of 4)
802… Action, SN=3859, FN=0, Flags=........
802… Action, SN=901, FN=0, Flags=........
EAP… Key (Message 2 of 4)
EAP… Key (Message 3 of 4)
EAP… Key (Message 4 of 4)
```

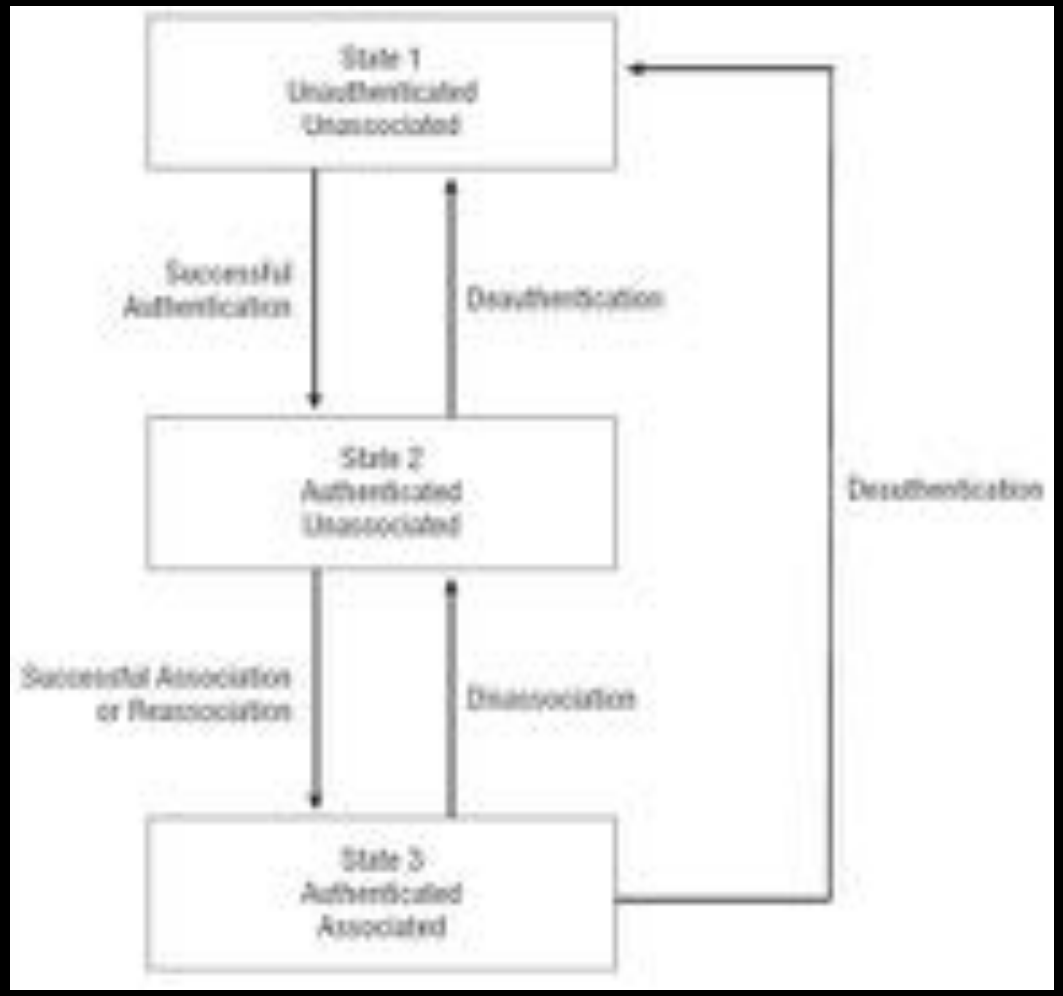
Demo

AD-LAB
AD LAB 5G

802.11 state machine

数据资源中心
Automotive Data Center

802.11 state machine detailed



- **State 1: A state that does not require too much interaction**

- **State 2: More types of packets are accepted**

- **State 3 : Keep connection and AP interacts with the STA**

数据资源中心
Automotive Data Center

What’s the difference between fuzz AP and fuzz STA?

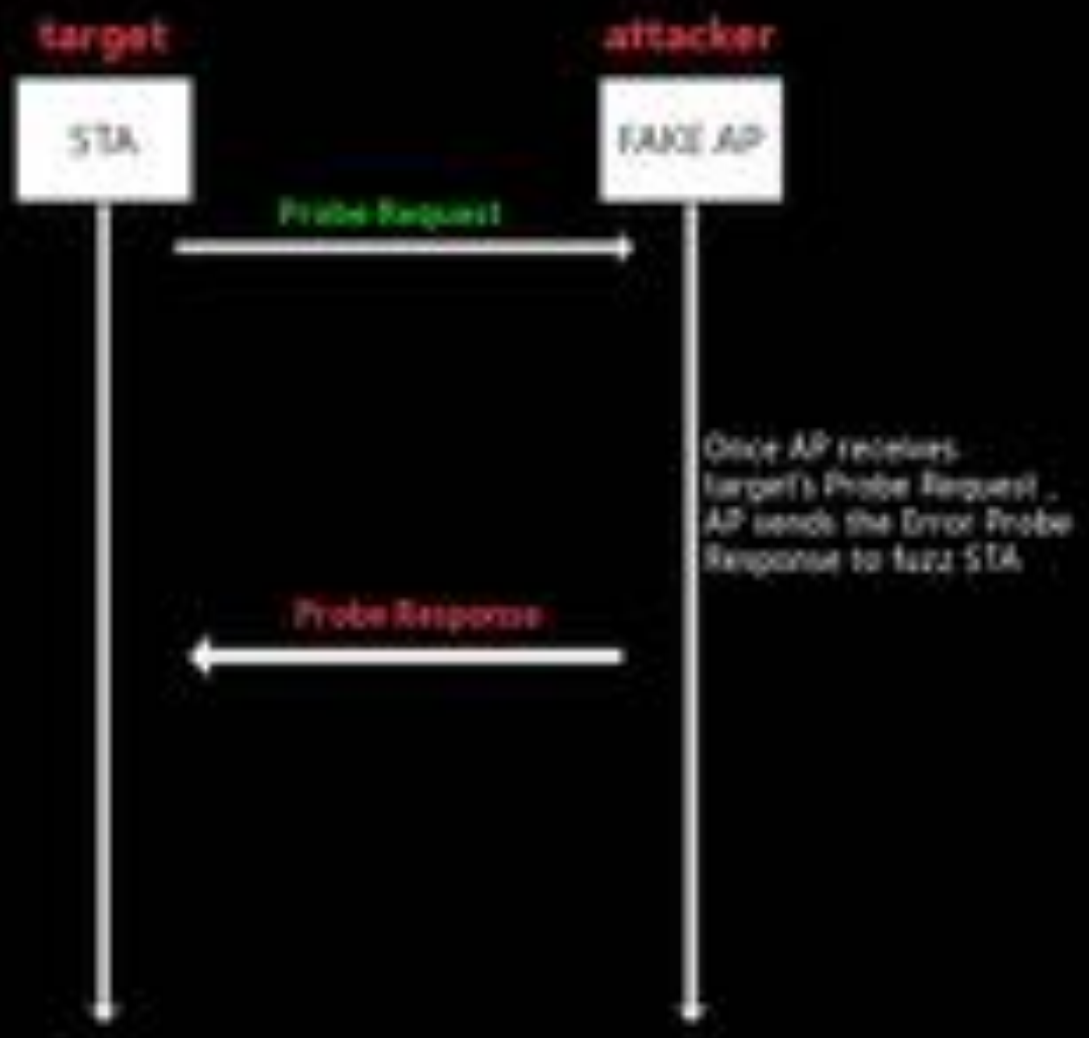
- Fuzz AP ----------> request frame

- **Fuzz STA** ----------> response frame

How to fuzz STA?

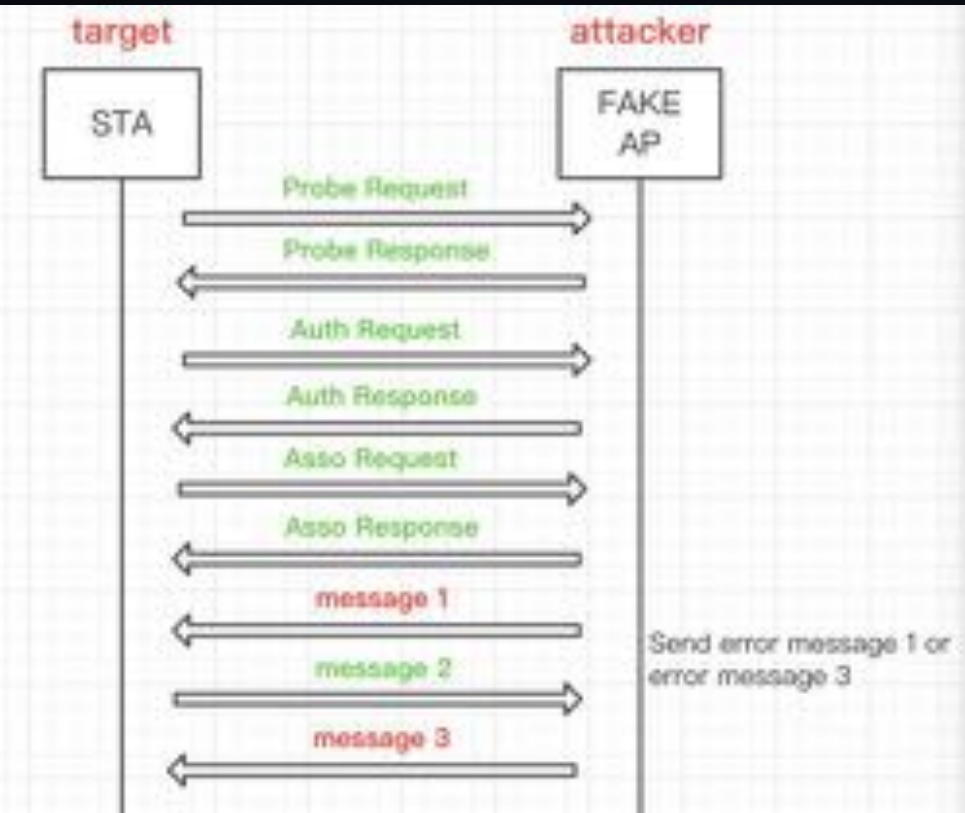
- FAKE AP: sniff and response

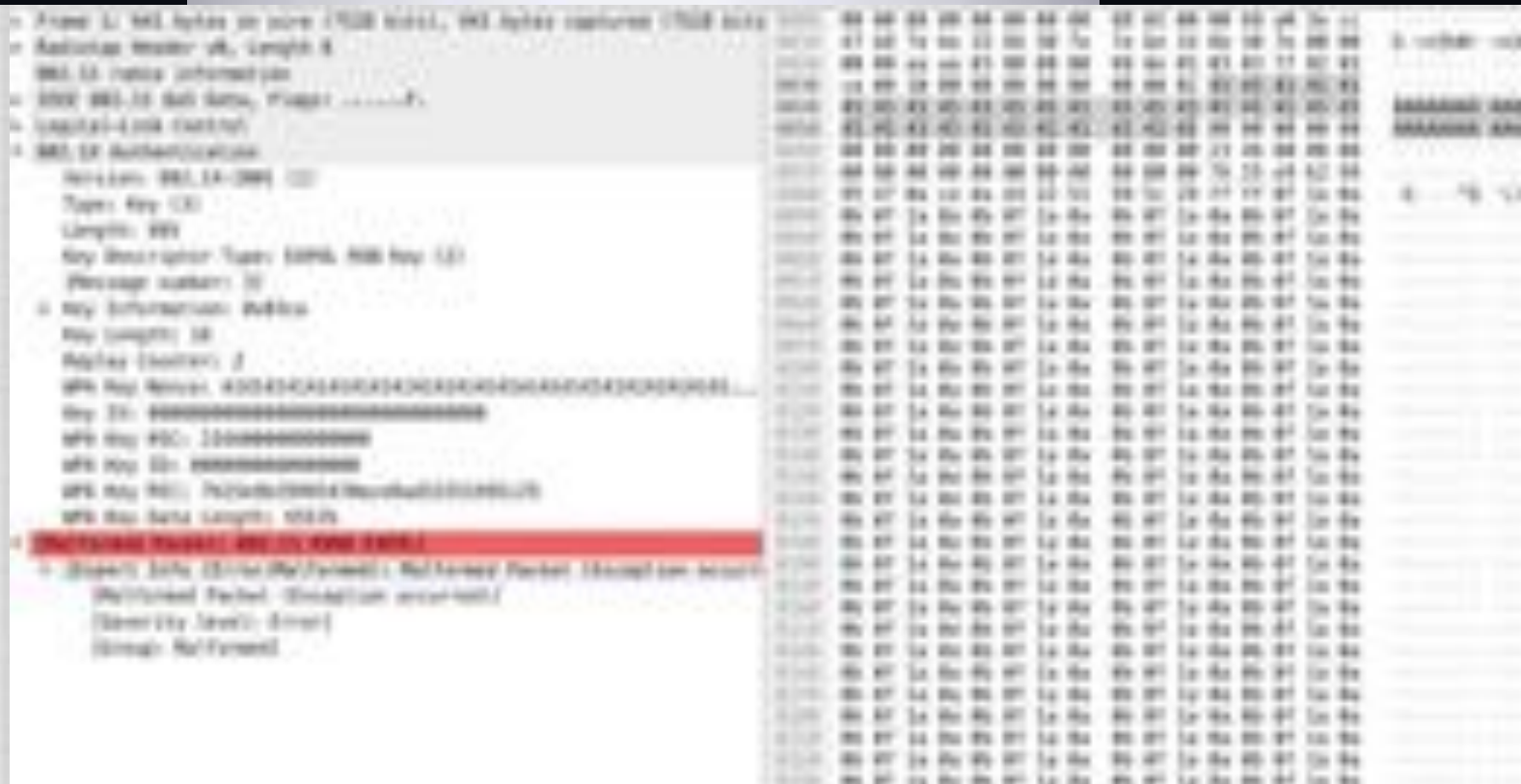
数据资源中心
Automotive Data Center

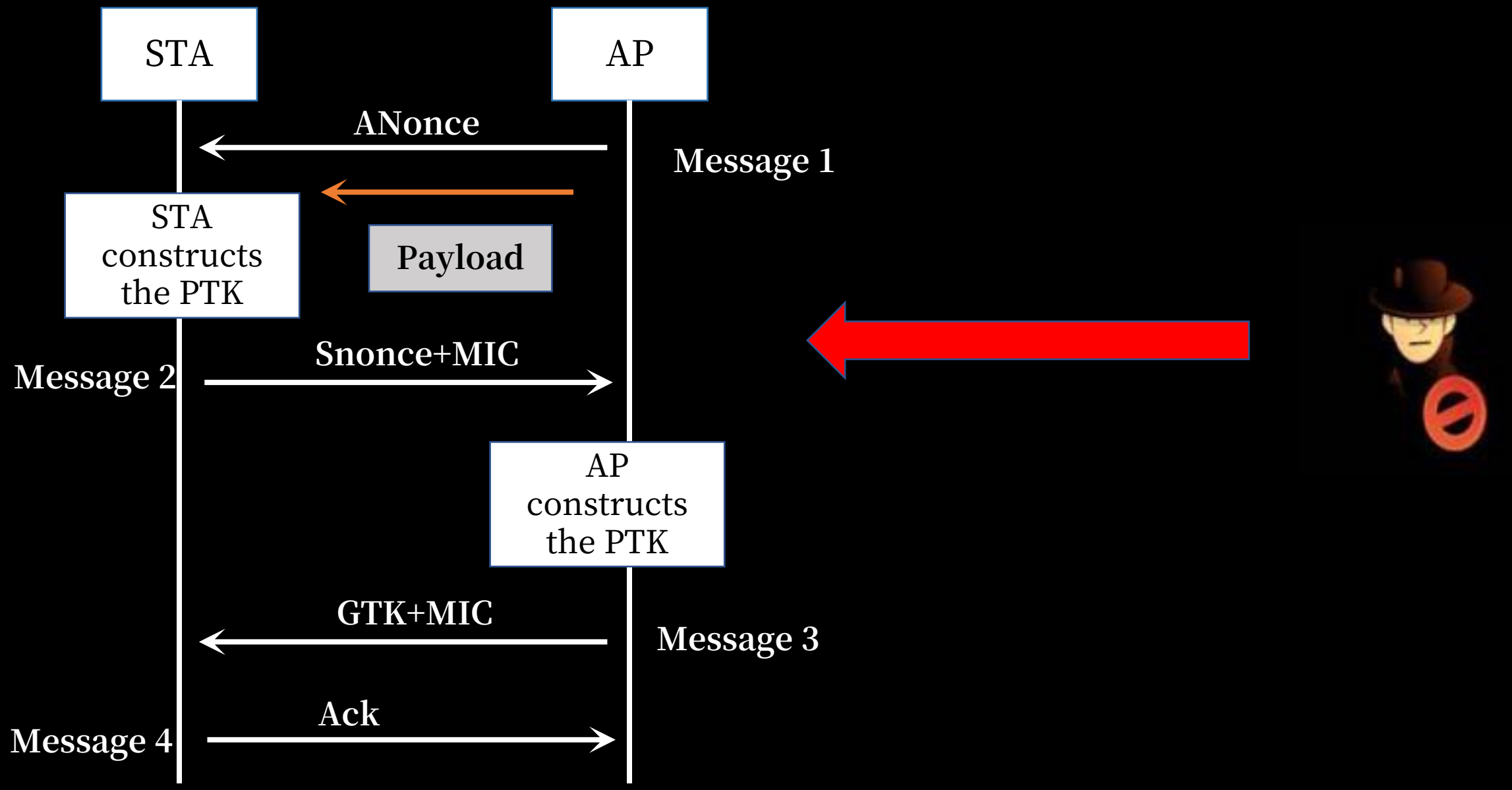


数据资源中心
Automotive Data Center

Attack HandShake







数据资源中心
Automotive Data Center

308	4.415850233	0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	802.11	32 Null function (No data),
309	4.416914598	0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	802.11	32 Null function (No data),
310	4.417099339		0a:0a:0a:0a:0a:0a (0a:0a…	802.11	28 Acknowledgement, Flags=.
311	4.418115471	0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	802.11	32 Null function (No data),
312	4.418211483		0a:0a:0a:0a:0a:0a (0a:0a…	802.11	28 Acknowledgement, Flags=.
313	4.418497108	Shenzhen_c1:62:c2	0a:0a:0a:0a:0a:0a	802.11	44 Deauthentication, SN=627
314	4.419326794	0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	802.11	32 Null function (No data),
315	4.420202878	0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	802.11	32 Null function (No data),
316	4.420949257	0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	802.11	32 Null function (No data),

Unusual attack

Shenzhen_c1:62:c2	0a:0a:0a:0a:0a:0a	EAPOL	151 Key (Message 1 of 4)
Shenzhen_c1:62:c2	0a:0a:0a:0a:0a:0a	EAPOL	151 Key (Message 1 of 4)
0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	EAPOL	163 Key (Message 2 of 4)
0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	EAPOL	168 Key (Message 2 of 4)
Shenzhen_c1:62:c2	0a:0a:0a:0a:0a:0a	EAPOL	207 Key (Message 3 of 4)
Shenzhen_c1:62:c2	0a:0a:0a:0a:0a:0a	EAPOL	207 Key (Message 3 of 4)
0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	EAPOL	141 Key (Message 4 of 4)
0a:0a:0a:0a:0a:0a	Shenzhen_c1:62:c2	EAPOL	146 Key (Message 4 of 4)

Demo

Conclusion

数据资源中心
Automotive Data Center

Q&A

Contact information

LiDong Li : wirelessdonghack@gmail.com

XianZi Kong : n3k0sec@gmail.com

数据资源中心
Automotive Data Center

THANKS

Happy Hackingg