

ABOUT US

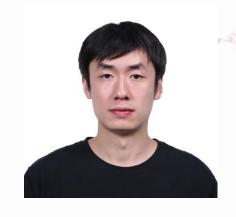


Xie Haikuo security researcher of Huawei Singularity Security Lab



Wang Ying security researcher of Baidu Security Lab X-Team.





OVERVIEW

- BACKGROUND
- ATTACK-SURFACE
- FUZZ
- VULNERABILITY
- CONCLUSIONS

BACKGROUND

- BACKGROUND
- ATTACK-SURFACE
- FUZZ
- VULNERABILITY
- CONCLUSIONS

BACKGROUND

Mainstream Vendors













BACKGROUND

WiFi Vulnerabilities

- 2017 Over The Air: Exploiting Broadcom's Wi-Fi stack
- 2017 Over The Air: Exploiting The Wi-Fi stack on Apple Devices
- 2018 RESERCHING MARVELL AVASTAR WI-FI:FROM ZERO KNOWLEDGE TO OVER-THE-AIR ZERO-TOUCH RCE
- 2019 Broadcom WiFi Driver Flaws Expose Computers, Phones, Iot to RCE Attacks. (CVE-2019-8564, CVE-2019-9500, CVE-2019-9501, CVE-2019-9503

•

- BACKGROUND
- ATTACK-SURFACE
- FUZZ
- VULNERABILITY
- CONCLUSIONS

1. Association stage Authentication 3. The other stage function

4. WiFi Driver IOCTL



Remote

Local

sta ap Beacon

Probe Request

Probe Response

Authentication Request

Authentication Response

> Association Request

> Association Response

Association stage

Beacon/Probe frame	STA obtains some basic information of AP, such as the name of hotspot, supported rate, supported authentication method and so on.
Authentication frame	Select authentication algorithm
Association frame	When STA association is successful, AP will return an association ID to identify this association

Association stage

sta





Beacon

Probe Request

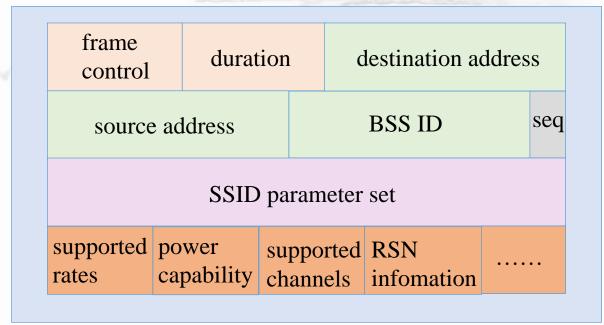
Probe Response

Authentication Request

Authentication Response

Association Request

Association Response



Frame header

Frame body

Association Request

Information Element

Element ID length Element ID Extension Information Element format

- 1. Variable length structure
- 2. Abundant IEs
- 3. Extension IEs
- 4. Private customized IEs. e.g. Vendor specific IE
- 5. Structure contains structure. e.g. RSN IE

sta ap Association Response EAPOL 1 EAPOL 2 EAPOL 3 EAPOL 4

Authentication stage

sta 📁

.

Association Response

EAPOL-start

EAP-Request/Identity

EAP-Response/Identity

EAP-Request(start)

EAP-Response(M1)

EAP-Request(M2)

EAP-Response(M3)

EAP-Request(M4)

EAP-Response(M5)

EAP-Request(M6)

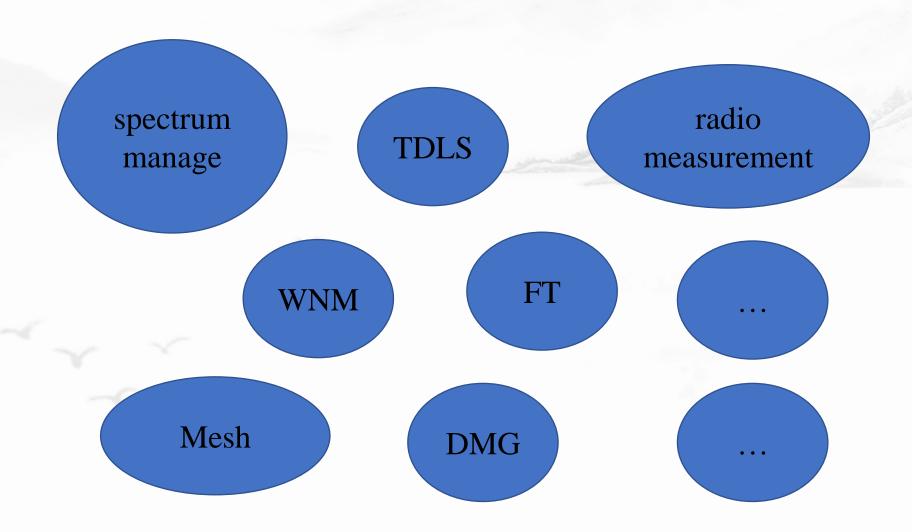
EAP-Response(M7)

EAP-Request(M8)

EAP-Response(Done)



The other function



FUZZ

- BACKGROUND
- ATTACK-SURFACE
- FUZZ
- VULNERABILITY
- CONCLUSIONS

FUZZ

Fuzz process

Fuzz mode

Mutation strategy

Sending frames

Crash detection

POC simplification

Vulnerability analysis

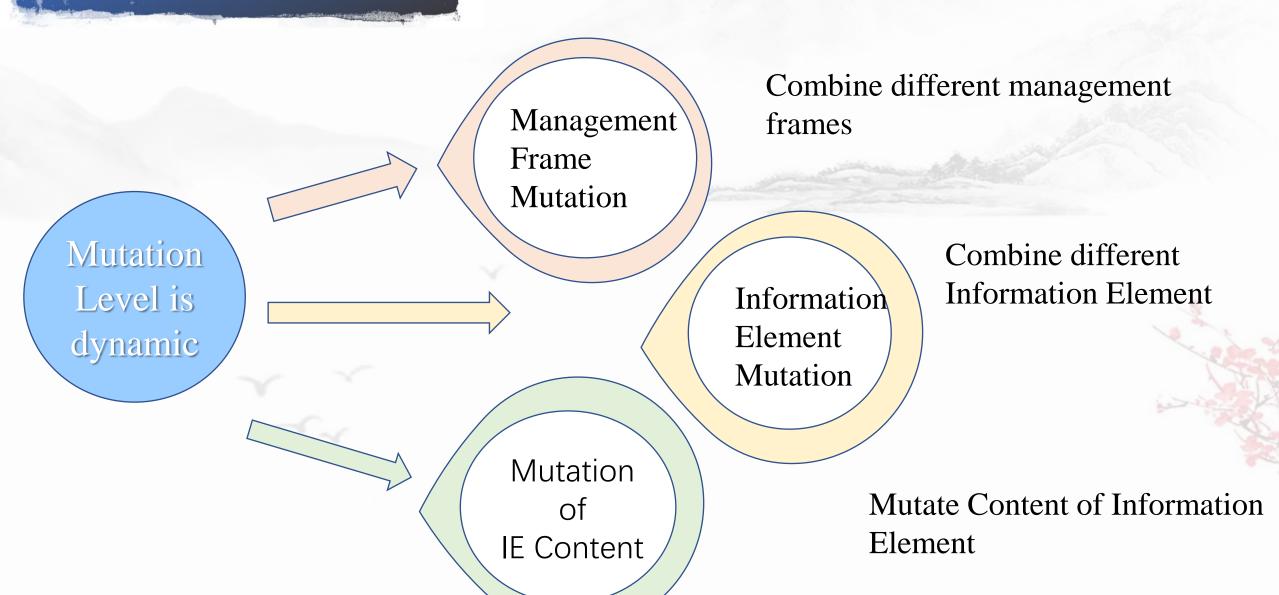


Fuzz mode

AP mode	STA mode	P2P mode				
1. WiFi Association stage						
2.	WiFi Authentication st	age				
~~~	3. The other function					

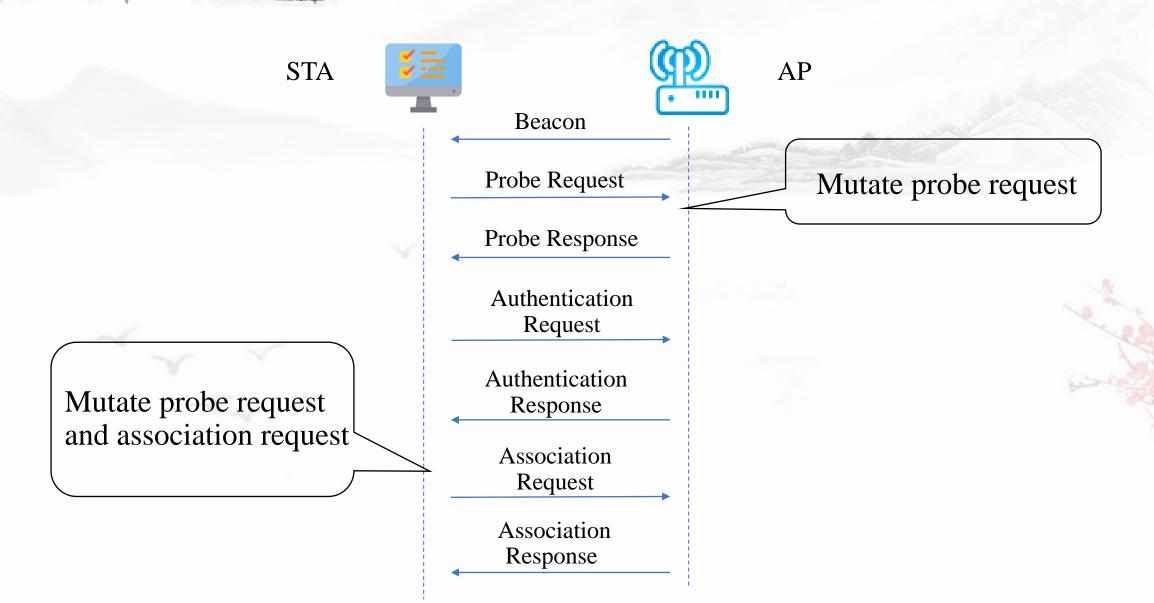
FUZZ

### **Mutation strategy**





### **Management Frame Mutation**





#### **Information Element Mutation**

tag id length data 802.11 IE frame duration destination address control **BSS ID** seq source address SSID parameter set supported power supported RSN capability rates channels infomation

**Association Request** 

**IE mutate randomly** 

Change a IE
Add a IE
Delete a IE

Different IEs mutate together

Change multiple IEs
Add multiple IEs
Delete multiple IE



### **Mutation of IE Content**

#### 802.11 IE -- RSN

Tag Number

Tag Length

RSN version

Group
Cipher Suit

Pairwise Cipher Suit Count

Pairwise Cipher Suit List

•••••

RSN capabilities

Group Cipher Suit OUI

Group Cipher Suit type

Pairwise Cipher Suit 1

. . . . . .

Pairwise Cipher Suit n

IE's field mutate randomly

e.g. Tag length
Group Cipher Suit
suite count

IE's fields mutate together

Group Cipher Suit + suite count

Pairwise Cipher Suit OUI

Pairwise Cipher Suit type



#### How to send frames

#### **TOOL**

Ralink RT2870/RT3070/RT5370

Atheros AR9271

SDR

```
root@ubuntu:/home/one# ifconfig wlxe84e064cf326 down
root@ubuntu:/home/one# iwconfig wlxe84e064cf326 mode monitor
root@ubuntu:/home/one# ifconfig wlxe84e064cf326 up
root@ubuntu:/home/one# iwconfig wlxe84e064cf326 channel 6
root@ubuntu:/home/one# iwconfig
wlxe84e064cf326 IEEE 802.11 Mode:Monitor Frequency:2.437 GHz Tx-Power=20 dB

M

Retry short long limit:2 RTS thr:off Fragment thr:off
Power Management:off

lo no wireless extensions.

ens33 no wireless extensions.
```

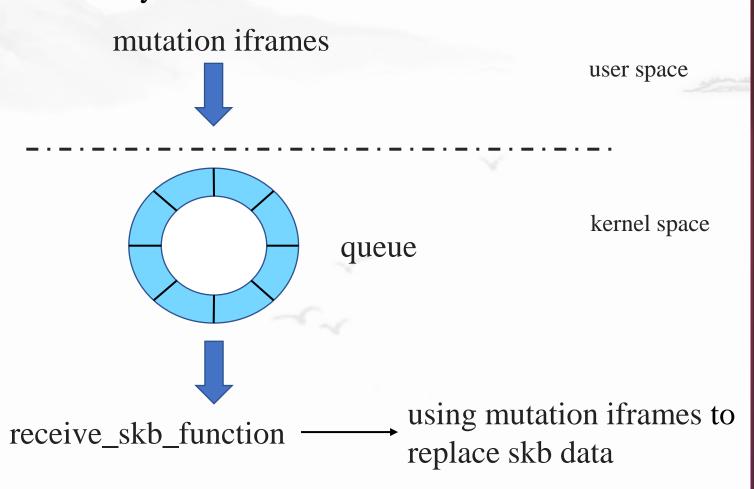


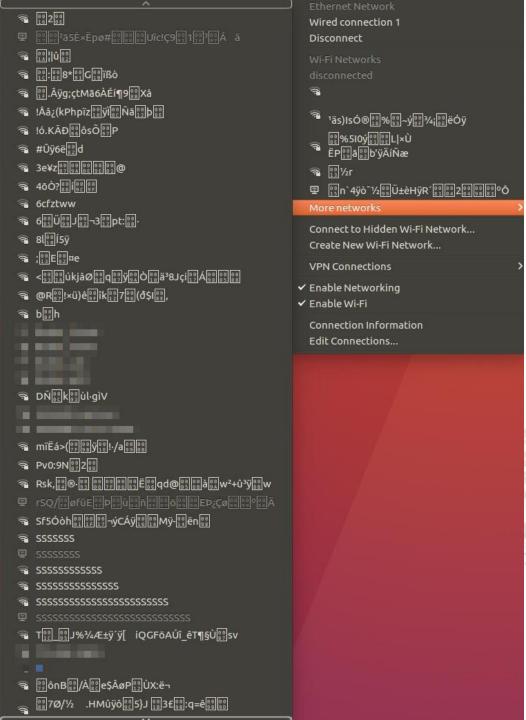




# FUZZ

In order to improve the efficiency of fuzzing, we can modify the code of WI-FI module in Linux.







### Vulnerability analysis

- Qualcomm Android open source code
- Old version driver symbol information
- Strings
- According to the frame and IE of trigger vulnerability and function calling stack

# FUZZ

No	CVE ID	Manufactur er	OS	Vulnerability	Upcoming
1	CVE-2020-0569	Intel	Windows	PCIE WiFi Driver netwtw04.sys Out-Of-Bound Write Vulnerability	Qualcomm
2	CVE-2020-0558	Intel	Windows	PCIE WiFi Driver netwtw06.sys Buffer Overflow Vulnerability	3
3	CVE-2020-0569	Intel	Windows	PCIE WiFi Driver netwtw06.sys Out-Of-Bound Write Vulnerability	Realtek
4	CVE-2020-0569	Intel	Windows	PCIE WiFi Driver netwtw08.sys Out-Of-Bound Write Vulnerability	8
5	CVE-2020-3650	Qualcomm	Windows	PCIE WiFi Driver athw10x.sys Buffer Overflow Vulnerability	
6	CVE-2020-3652	Qualcomm	Windows	PCIE WiFi Driver athw10x.sys Out-Of-Bound Read Vulnerability	
7	CVE-2020-3653	Qualcomm	Windows	PCIE WiFi Driver Qcamain10x64.sys Out-Of- Bound Read Vulnerability	

- BACKGROUND
- ATTACK-SURFACE
- FUZZ
- VULNERABILITY
- CONCLUSIONS

### CVE-2020-3650

### Qualcomm ATHW10X.SYS Driver Stack-Overflow Vulnerability

### CVE-2020-3650

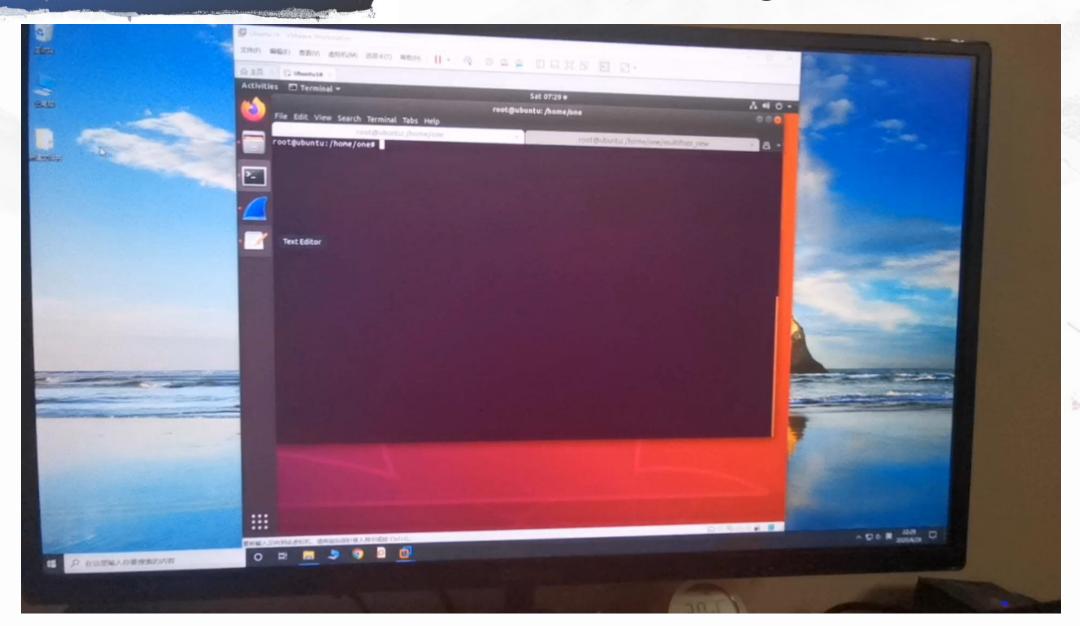
- SupportedRates IE and ExtenedSupportedRates IE
- Probe\Association Request\Response frame with malformed supportedrates ie and malformed extendedsupportedrates ie

```
Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag Number: Supported Rates (1)
    Tag length: 8
    Supported Rates: 6(B) (0x8c)
    Supported Rates: 9 (0x12)
    Supported Rates: 12(B) (0x98)
    Supported Rates: 18 (0x24)
    Supported Rates: 24(B) (0xb0)
    Supported Rates: 36 (0x48)
    Supported Rates: 48 (0x60)
0040 62 2d 41 6e 64 72 6f 69 64 5f 64 63 62 37 01 08 b-Androi d_dcb7...
0050 8c 12 98 24 b0 48 60 6c 03 01 01 05 04 01 02 00 ...$.H`l ......
```

### **Vulnerability logic**

```
void function(BYTE *Rates,BYTE *ExtendedRates)
      if( Rates[1] > 36)
                printf("Bad rates len");
                return -1;
      if (Rates[1] + ExtendedRates[1] > 36 && Rates[1] < 36)
                printf("extended rate set too large");
                return -1;
      memcpy(..);
```

### **DEMO**



### CVE-2020-0558

Out-Of-Bound Write Vulnerabilities in All family of Intel dual-band wireless adapters

### CVE-2020-0558

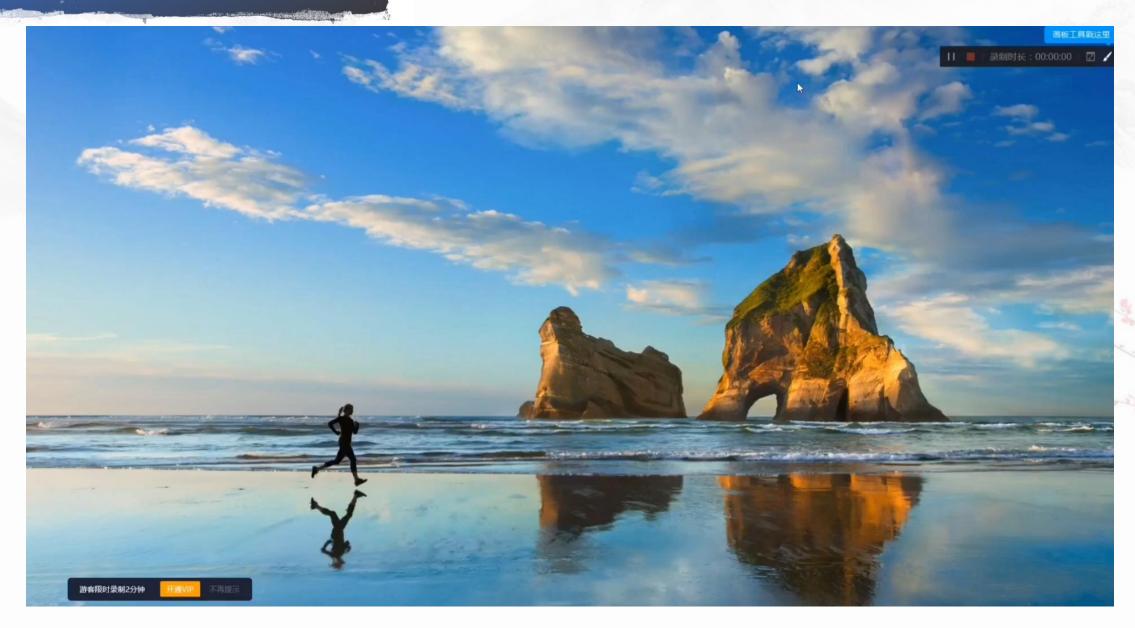
- * Netwbw02.sys for Intel® Dual Band Wireless-N 7260
- * Netwtw04.sys for Intel® Dual Band Wireless-AC 3168
- * Netwtw06.sys for Intel® Dual Band Wireless-AC 8265
- * Netwtw08.sys for Intel® Dual Band Wireless-AC 9260/AX200

### Vulnerability logic

SupportedOperationalClasses IE

```
void prvPanCnctProcessAssocSupportedChannelList()
      for(int i = 0;i < classesie[1];<math>i++)
             utilRegulatoryClassToChannelList()
```

### **DEMO**



### CONCLUSION

- BACKGROUND
- ATTACK-SURFACE
- FUZZ
- VULNERABILITY
- CONCLUSIONS

# CONCLUSION

- Threat is Expanding
- Focus on WiFi Password authentication stage and WiFi authenticated function

# Thanks

blackhat ASIA 2020

BRIEFINGS