WIFI-Important Remote Attack Surface: Threat is Expanding

ABOUT US

Xie Haikuo
security researcher of Huawei Singularity Security Lab

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

Zhang Ye
security researcher of Baidu Security Lab X-Team.

OVERVIEW

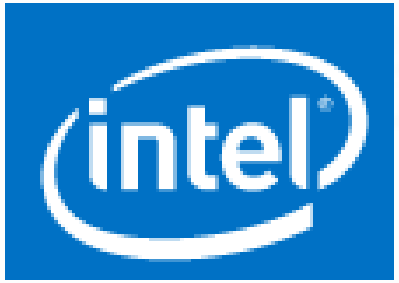
- BACKGROUND
- ATTACK-SURFACE
- FUZZ
- VULNERABILITY
- CONCLUSIONS

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
- ……

ATTACK-SURFACE

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

ATTACK-SURFACE

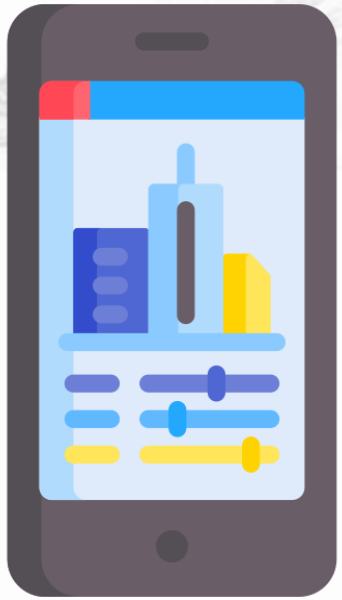
1. Association stage

2. Authentication stage

3. The other function

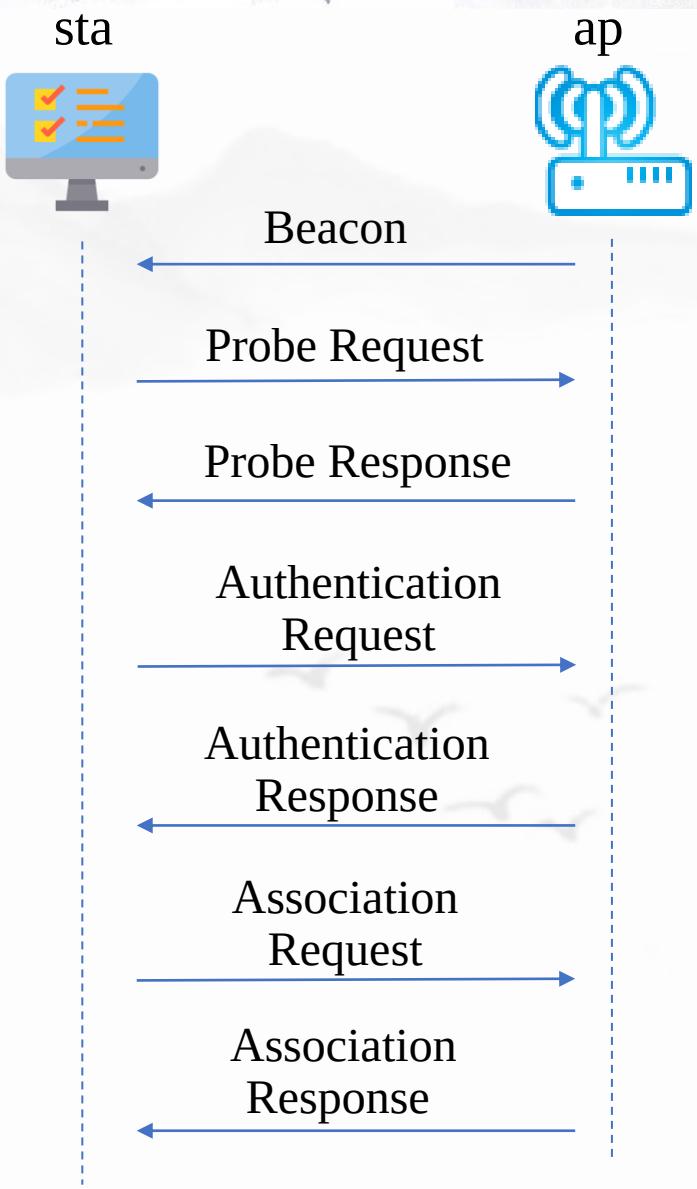
Remote

4.WiFi Driver IOCTL



Local

ATTACK-SURFACE

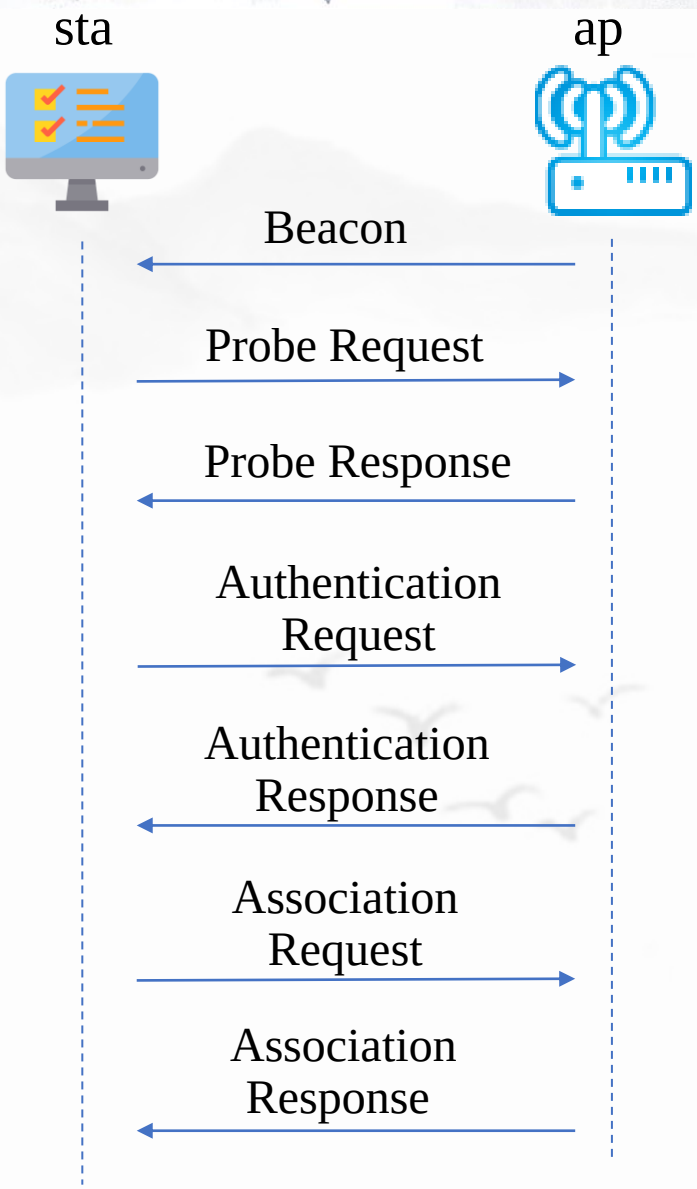


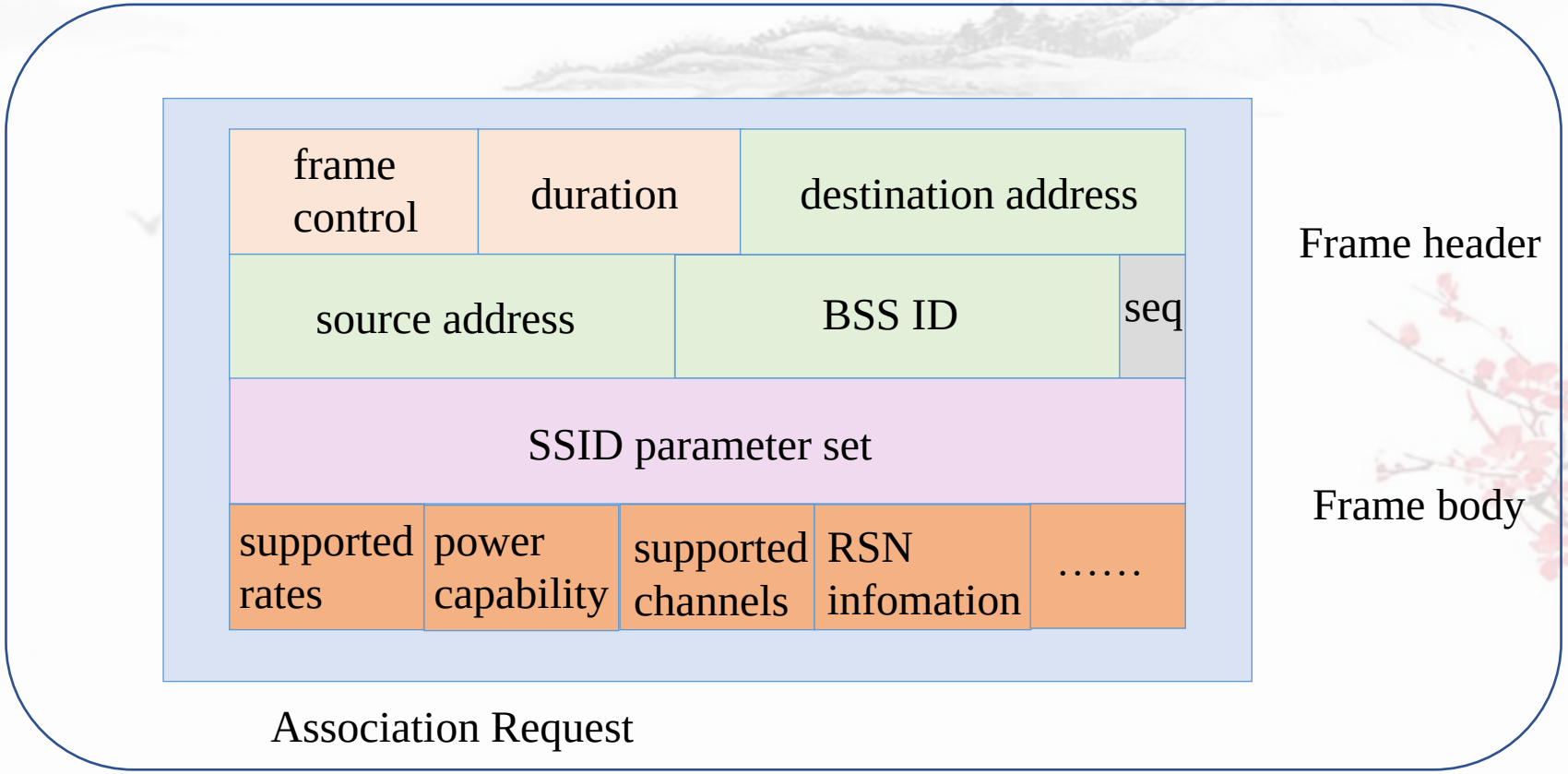
Association stage

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

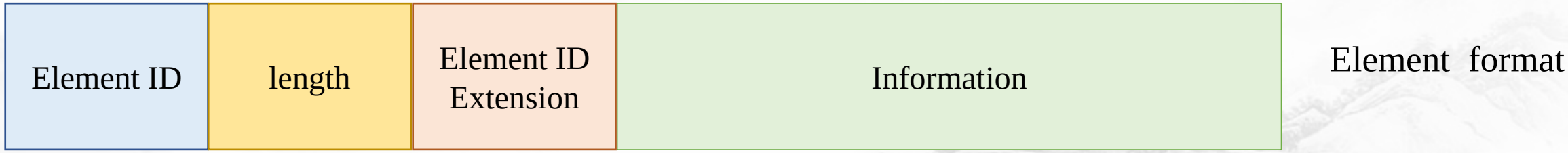
ATTACK-SURFACE

Association stage





Information Element



Element format

1. Variable length structure

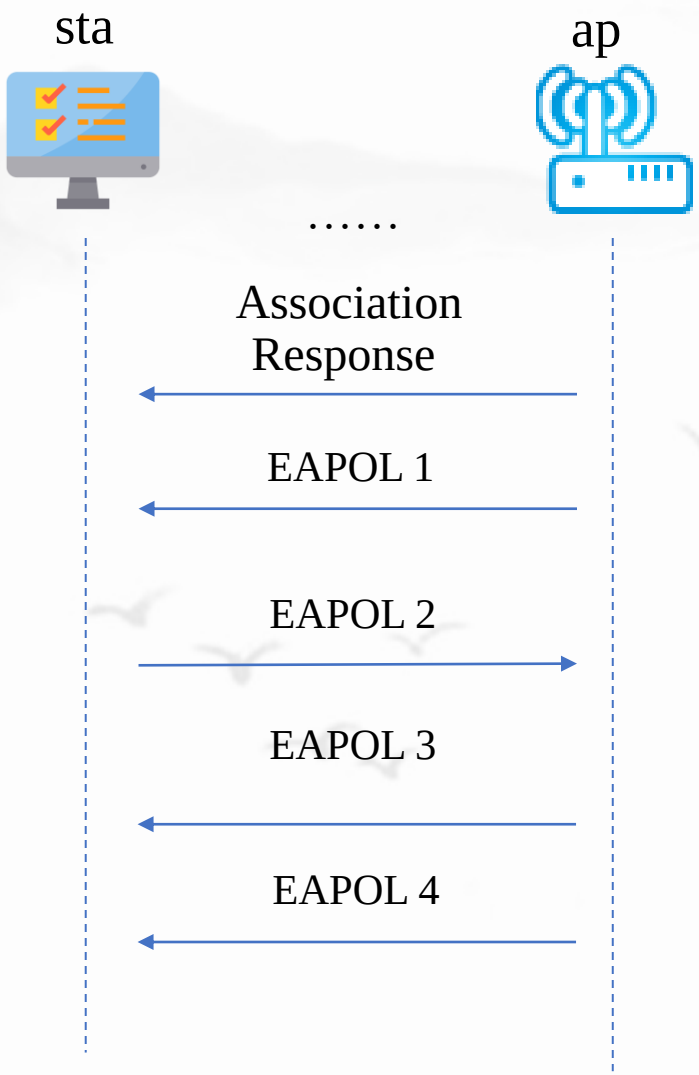
2. Abundant IEs

3. Extension IEs

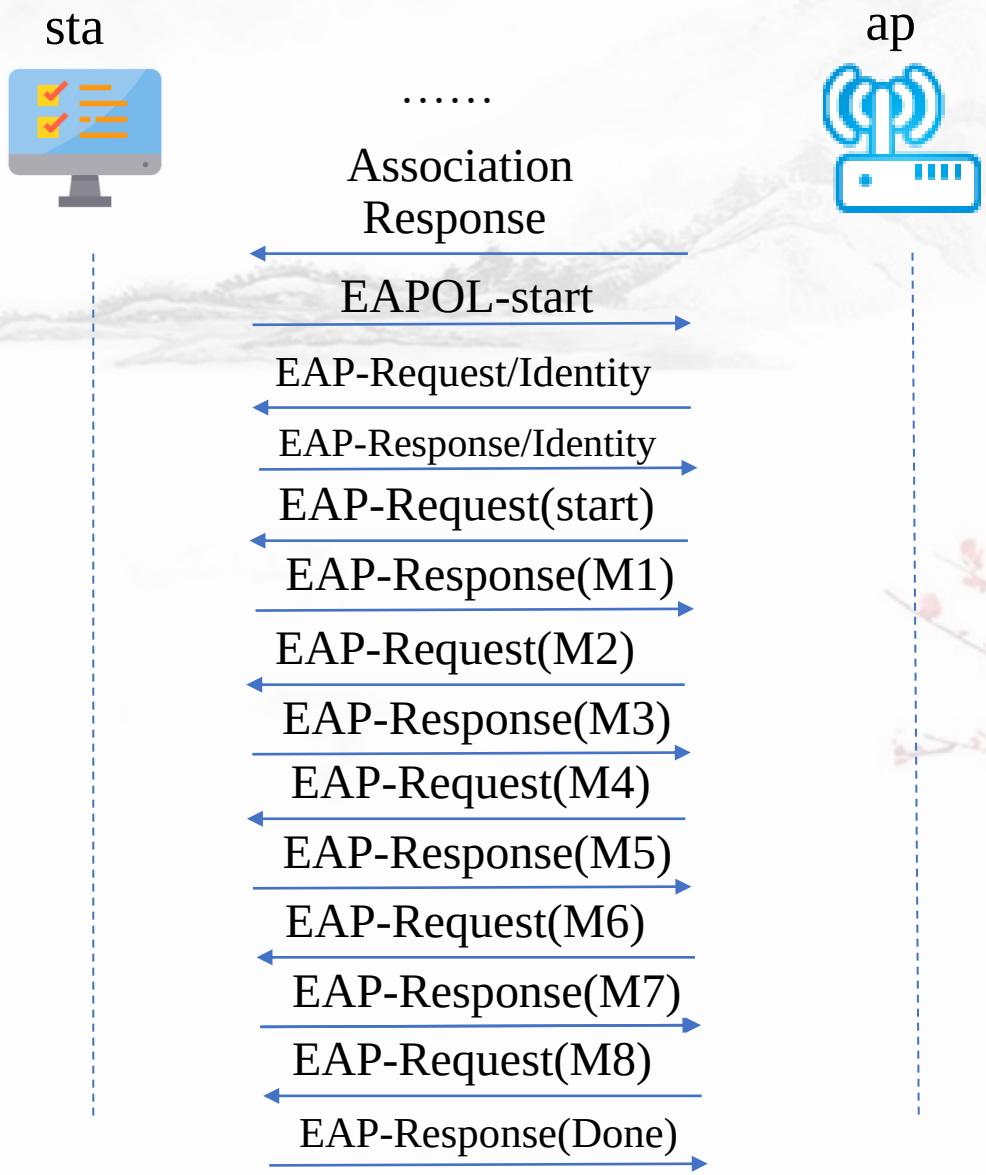
4. Private customized IEs. e.g. Vendor specific IE

5. Structure contains structure. e.g. RSN IE

ATTACK-SURFACE

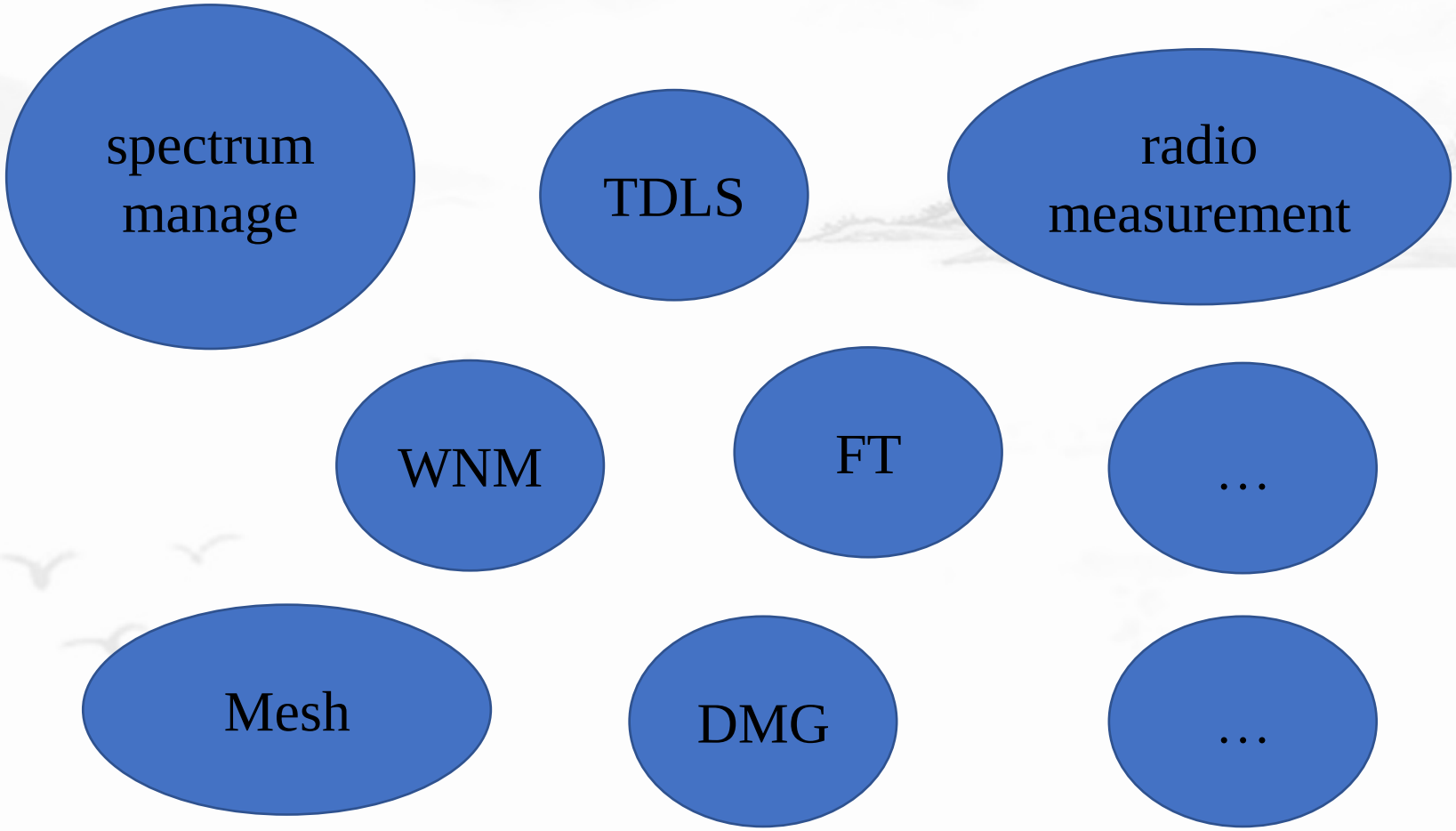


Authentication stage



ATTACK-SURFACE

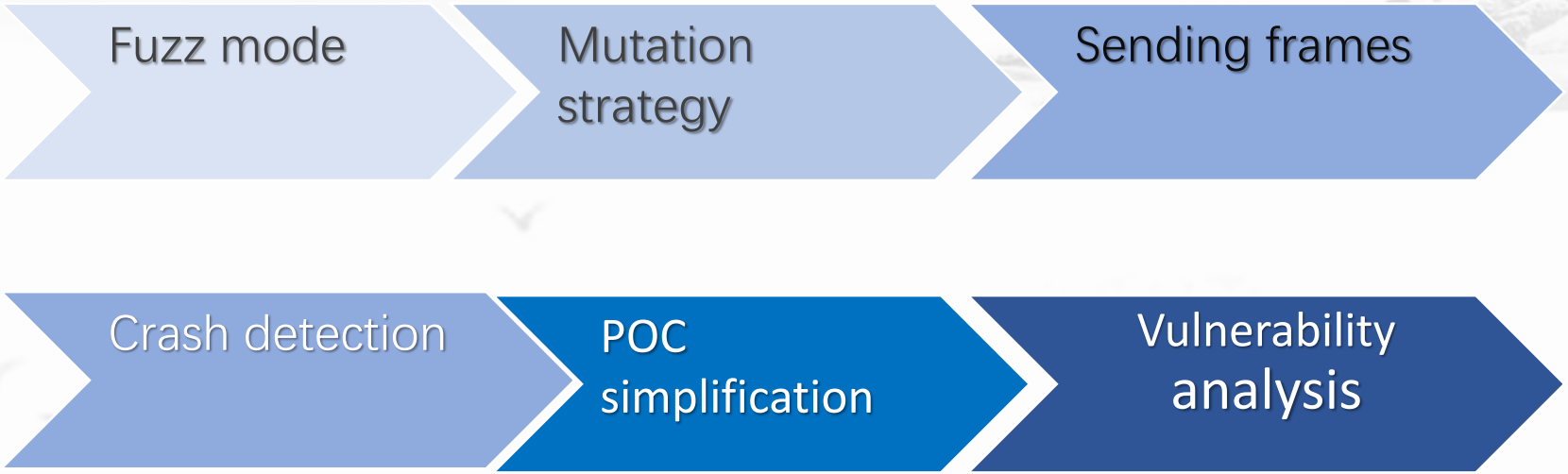
The other function



FUZZ

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

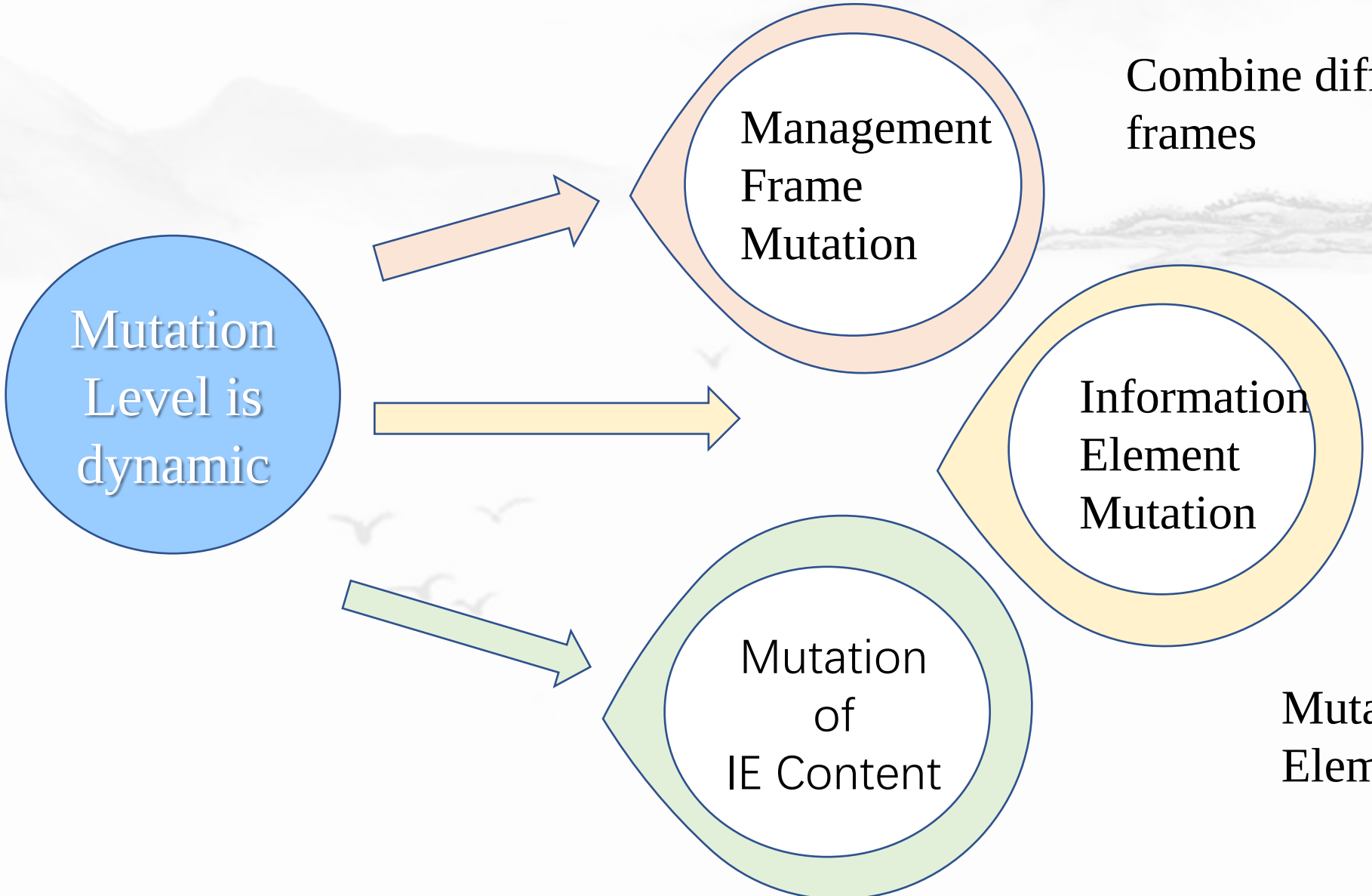
Fuzz process



Fuzz mode

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

Mutation strategy

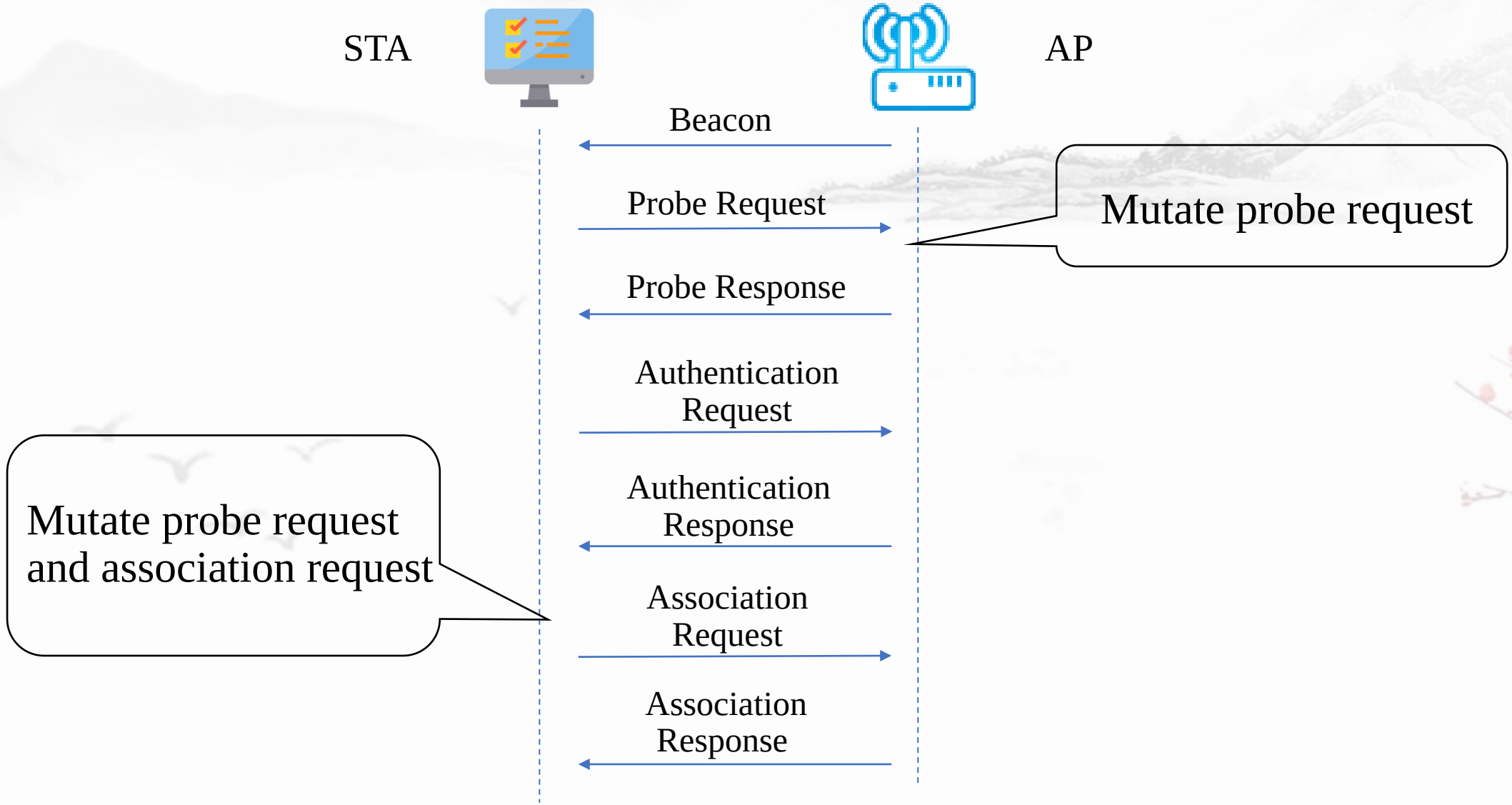


Combine different management frames

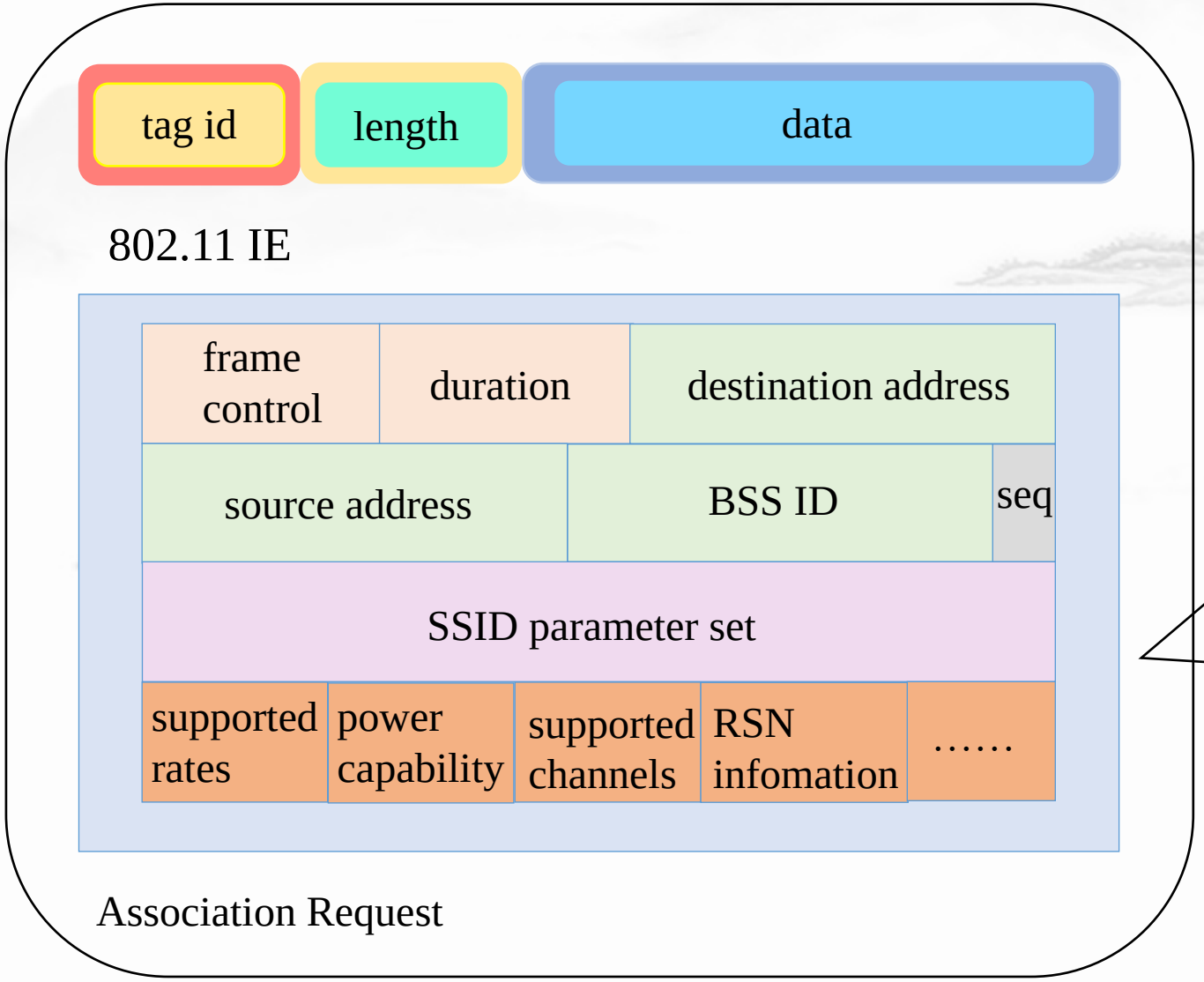
Combine different Information Element

Mutate Content of Information Element

Management Frame Mutation



Information Element Mutation



IE mutate randomly

- Change a IE
- Add a IE
- Delete a IE

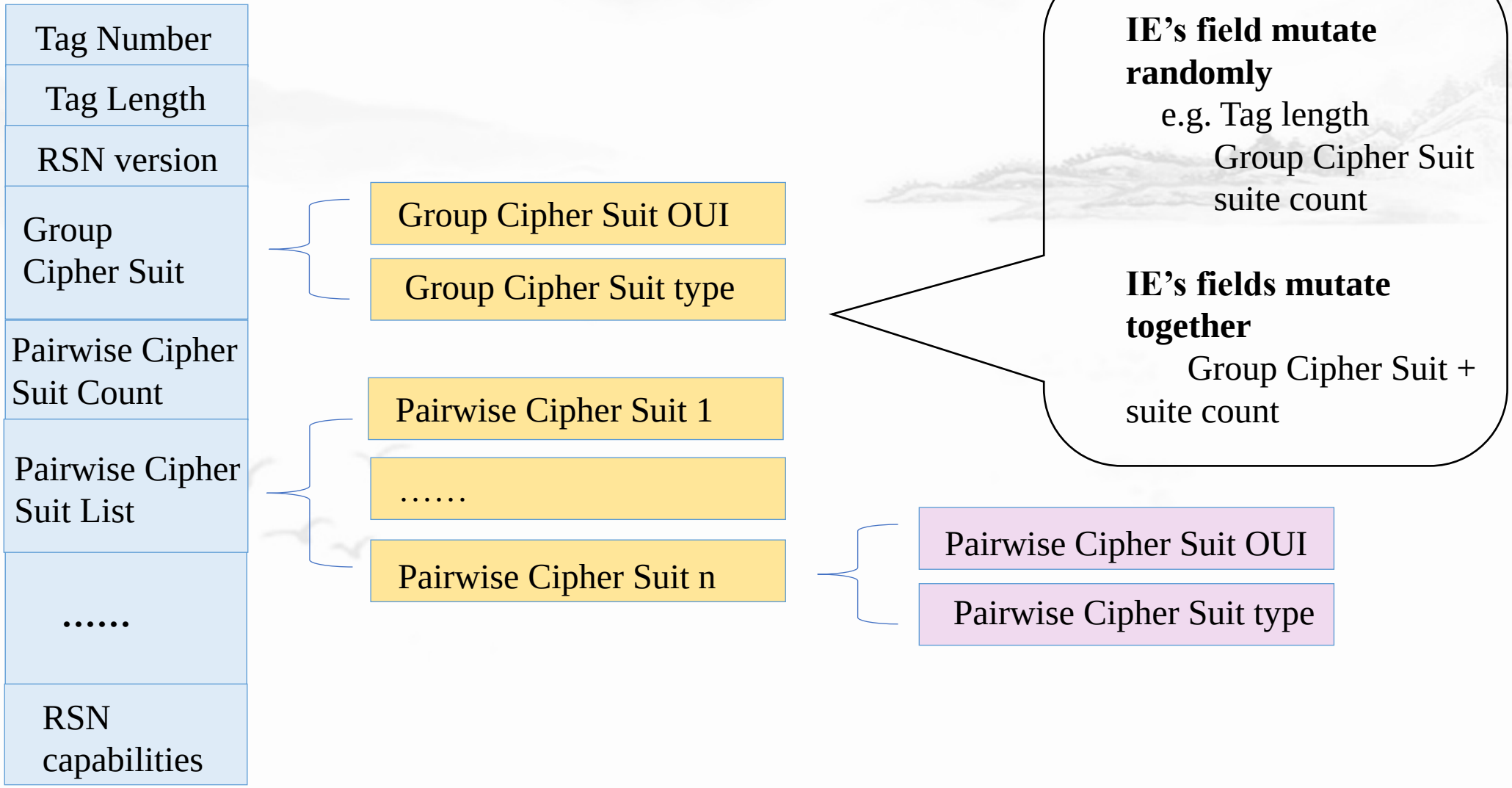
Different IEs mutate together

- Change multiple IEs
- Add multiple IEs
- Delete multiple IE

FUZZ

Mutation of IE Content

802.11 IE -- RSN



FUZZ

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.
```

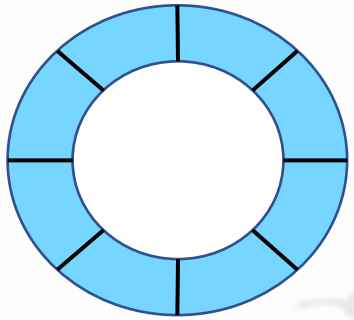
FUZZ

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

mutation iframes

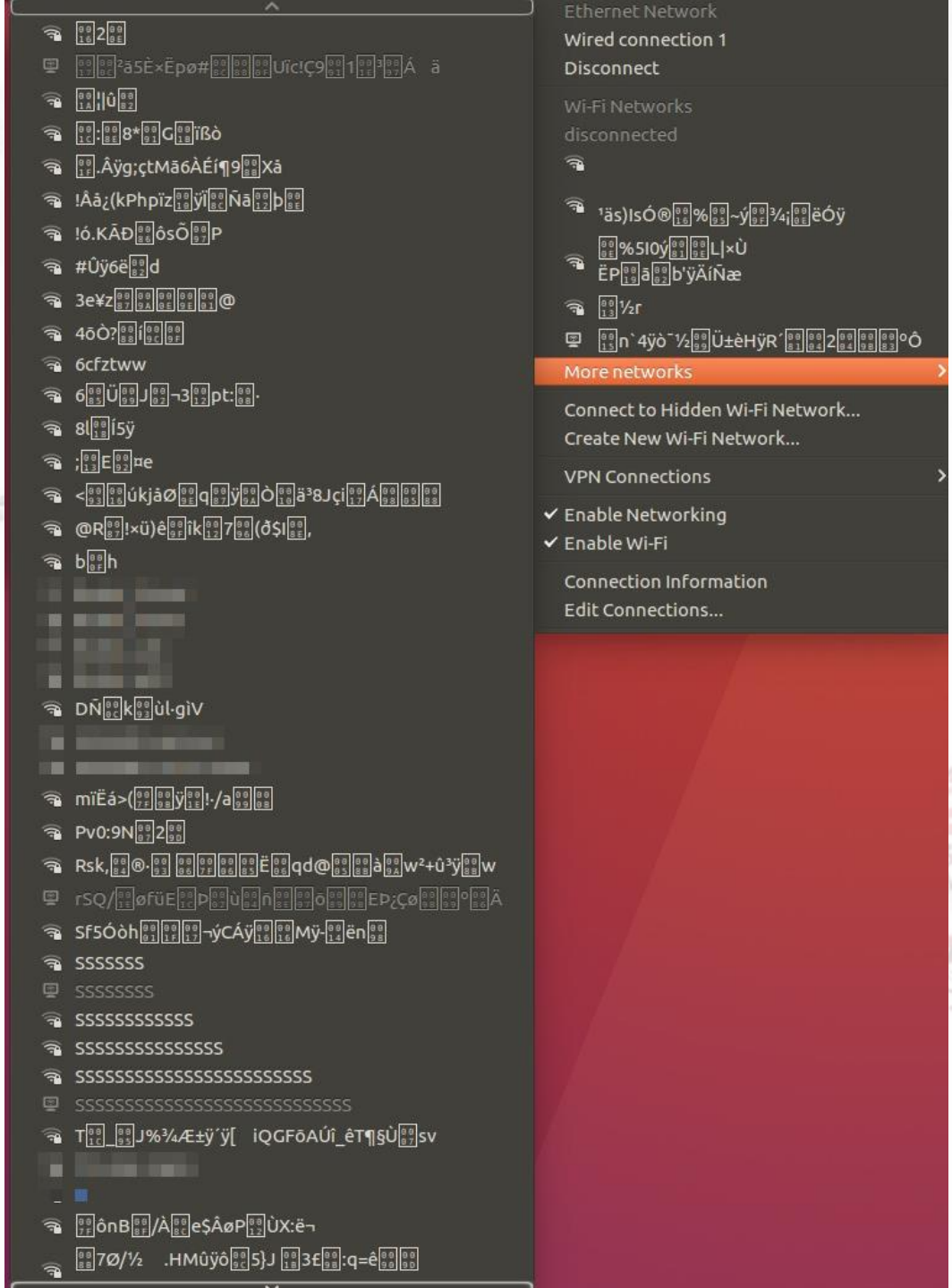
user space

kernel space



queue

receive_skb_function → using mutation iframes to replace skb data



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	Manufacturer	OS	Vulnerability
1	CVE-2020-0569	Intel	Windows	PCIE WiFi Driver netwtw04.sys Out-Of-Bound Write Vulnerability
2	CVE-2020-0558	Intel	Windows	PCIE WiFi Driver netwtw06.sys Buffer Overflow Vulnerability
3	CVE-2020-0569	Intel	Windows	PCIE WiFi Driver netwtw06.sys Out-Of-Bound Write Vulnerability
4	CVE-2020-0569	Intel	Windows	PCIE WiFi Driver netwtw08.sys Out-Of-Bound Write Vulnerability
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

Upcoming
Qualcomm
3
Realtek
8

VULNERABILITY

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

VULNERABILITY

CVE-2020-3650

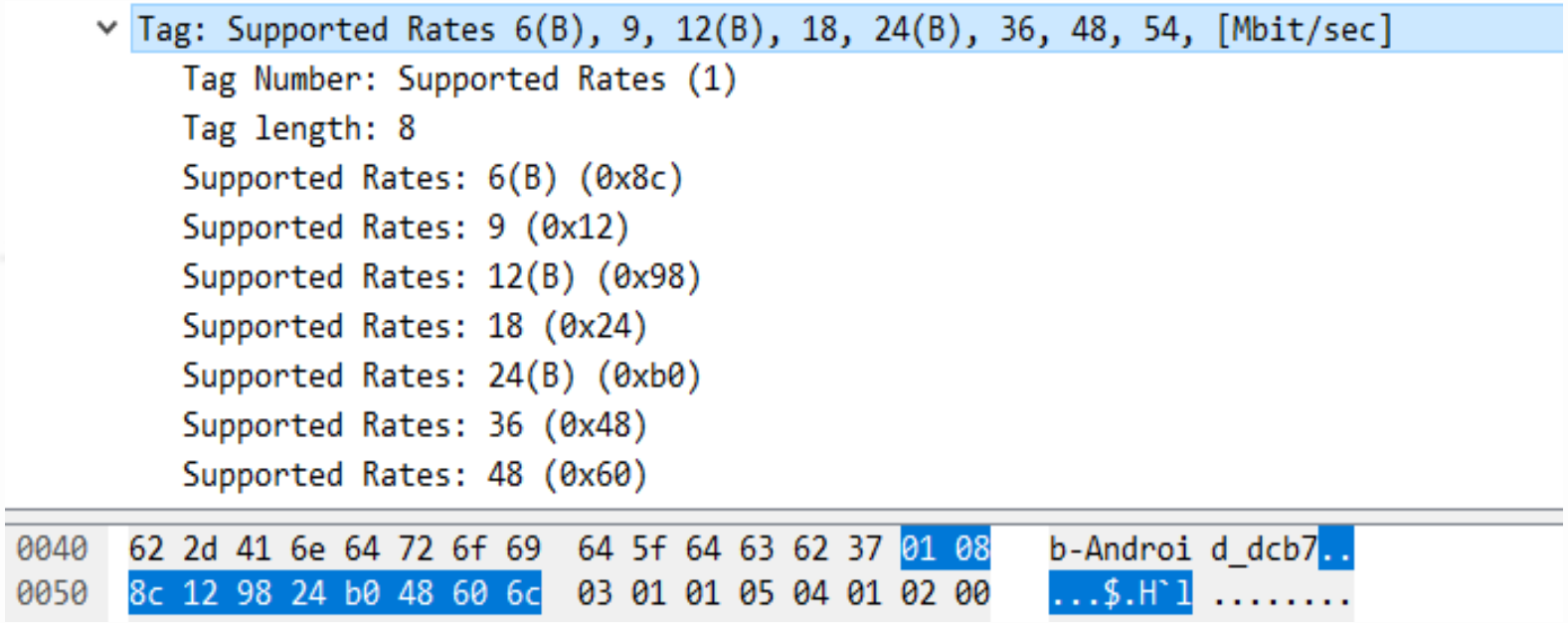
Qualcomm ATHW10X.SYS Driver Stack-Overflow Vulnerability

VULNERABILITY

CVE-2020-3650

- SupportedRates IE and ExtenedSupportedRates IE

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



VULNERABILITY

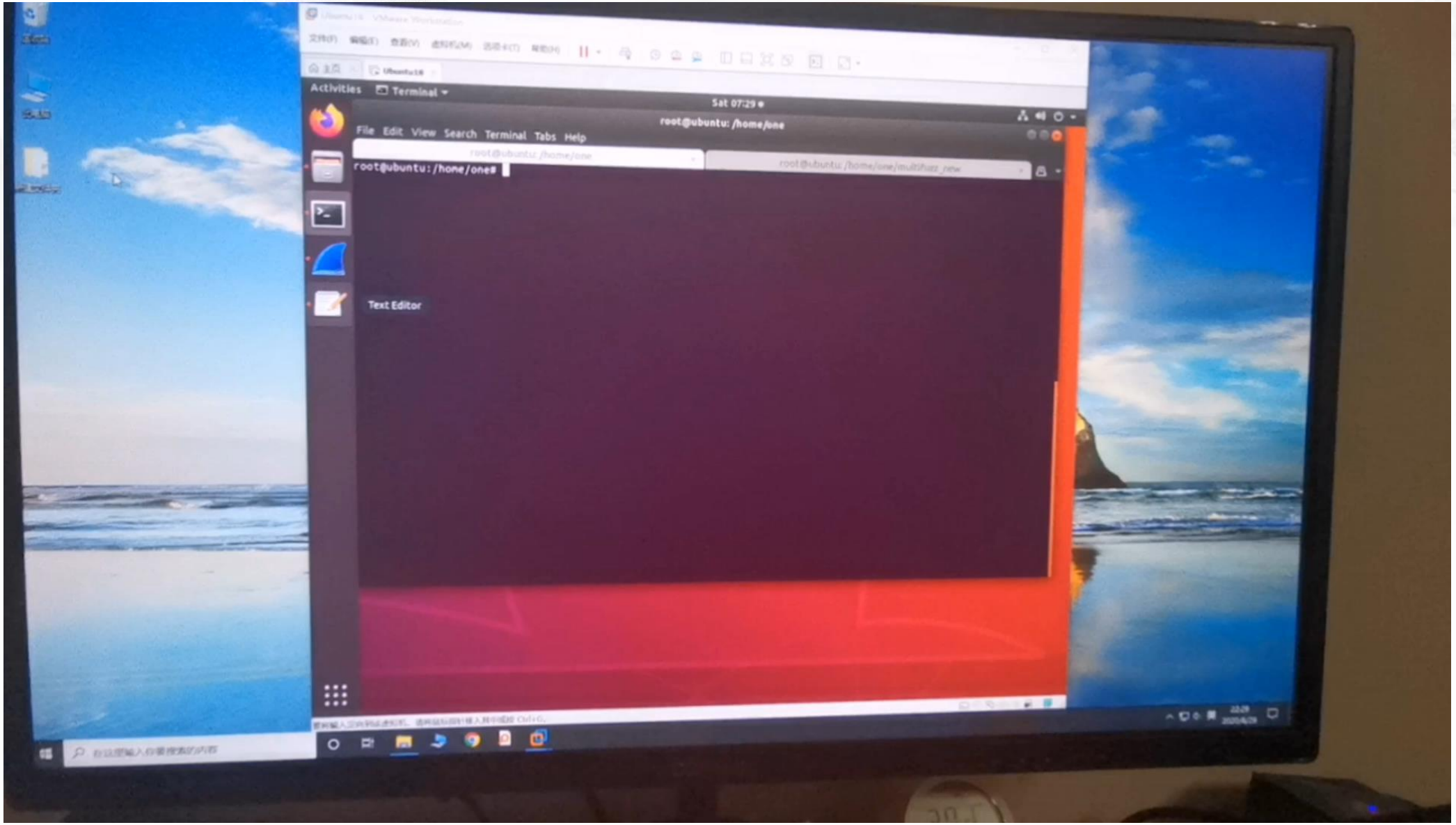
Vulnerability logic

```
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(..);


}
```

VULNERABILITY

DEMO



VULNERABILITY

CVE-2020-0558

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

VULNERABILITY

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];i++)
        {
                utilRegulatoryClassToChannelList()
                ...
        }
        ...
}
```

VULNERABILITY

DEMO

CONCLUSION

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

CONCLUSION

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

Thanks