FragAttacks: Recent Flaws in WPA2/3 and New Defenses

GISEC, 21 March ‘22, Dubai

Prof. dr. Mathy Vanhoef
Advancements in Wi-Fi security

› WPA3 is continuously being updated
  » Preventing Dragonblood attack
  » Securing hotspots
Advancements in Wi-Fi security

- WPA3 is continuously being updated
  - Preventing Dragonblood attack
  - Securing hotspots
- Operating channel validation
- Beacon protection
- KRACK patches proven secure

Despite these major advancements, we found flaws in all Wi-Fi networks (incl. WPA2/3)
Design flaws

Implementation Flaws
Implementation Flaws

Aggregation

Mixed key
Fragment cache
Background

Sending small frames causes high overhead:

```
header packet1 ACK header packet2 ACK ...
```

This can be avoided by **aggregating frames**:

```
header’ packet1 packet2 ... ACK
```
Background

Sending small frames causes high overhead:

This can be avoided by **aggregating frames**:

**Problem:** how to recognize aggregated frames?
Aggregation design flaw

<table>
<thead>
<tr>
<th>header</th>
<th>aggregated?</th>
<th>encrypted</th>
</tr>
</thead>
<tbody>
<tr>
<td>False</td>
<td></td>
<td></td>
</tr>
<tr>
<td>True</td>
<td>metadata</td>
<td>packet1</td>
</tr>
</tbody>
</table>
Aggregation design flaw

- Not authenticated
- header aggregated? encrypted
  - False
  - True metadata packet1 metadata packet2

Flip flag → payload is parsed differently → inject packets
Exploit steps

1. Get image from attacker’s server
2. Send special IPv4 packet
Exploit steps

1. Get image from attacker’s server
2. Encrypt as normal frame
3. Send special IPv4 packet
Exploit steps

1. Get image from attacker’s server
2. Set aggregated flag
3. Encrypt as normal frame
4. Send special IPv4 packet
Exploit steps

1. Get image from attacker’s server
2. Set aggregated flag
3. Encrypt as normal frame
4. Send special IPv4 packet
5. Encrypt as normal frame
6. Set aggregated flag
7. Inject any packet → **Inject ICMPv6 RA with malicious DNS server**
DEMO
Design flaws

Implementation Flaws
Trivial frame injection

Plaintext frames wrongly accepted:

› Depending if fragmented, broadcasted, or while connecting
Trivial frame injection

Plaintext frames wrongly accepted:

› Depending if fragmented, broadcasted, or while connecting
› Sometimes frames that resemble a handshake message
› Examples: Apple and some Android devices, some Windows dongles, home and professional APs, and many others!

→ Can trivially inject frames
DEMO
Design flaws

- Plaintext frames
- Broadcast fragments
- EAPOL forwarding
- Cloacked A-MSDUs
- Mixed fragments
- Out of order frag
- No fragmentation support
No fragmentation support

Some devices don’t support fragmentation

› But they treat fragmented frames as full frames
› Examples: OpenBSD and Espressif chips

→ Abuse to inject frames under right conditions
→ All devices are vulnerable to one or more flaws
Created tool to test devices

Has 45+ test cases for both clients and APs:

→ Available at https://github.com/vanhoofm/fragattack
Abusing design flaws requires multi-channel MitM

AP is cloned on **different channel**

Handshake succeeds & can reliably manipulate frames!
Channel validation

**Verify operating channel** when connecting to a network

Also need to handle some edge cases:

› After the clients wakes up from sleep mode
› When the network switches channel due to radar detection

→ Implemented on **Linux & Android**
Channel validation

› Collaborated with industry (Broadcom and Intel) to standardize the defense

› Now part of the latest update to the IEEE 802.11 standard
Channel validation

- Collaborated with industry (Broadcom and Intel) to standardize the defense
- Now part of the latest update to the IEEE 802.11 standard
- Recognized as an optional feature of WPA3
- Good initial step, hopefully becomes mandatory in future
Other defenses for Wi-Fi networks

Channel validation
Mitigates prerequisite of several recent attacks

Beacon protection
Authenticate beacons to prevent denial of service

› Both implemented on Linux and Android
› Now part of the **IEEE 802.11 standard**
› Wi-Fi Alliance is encouraging its adoption
Conclusion

› Discovered three **design flaws**
› Multiple **implementation flaws**
› Several flaws are **trivial to exploit**
› More info: [www.fragattacks.com](http://www.fragattacks.com)