FragAttacks are short for something called fragmentation and aggregation attacks. This is an attack that impacts all security protocols, even that of the new WPA3. This specifically has to do with the fragment and aggregation frames that exist within the standard frames used by wireless routers. The attacker can use these frames to either tick a victim into using a malicious DNS server or forge frames to try and procure data.

Allowing injection of packets can either be directed at a client or an access point. If directed toward a client, it can be manipulated into using a poisoned DNS server. However, against the access point could allow the attack to bypass the NAT and connect to devices within the LAN. Even though this sounds incredibly malevolent for users it can only occur if a user interacts with the attack or using network settings that wouldn’t be set as standard on any home machine.

The research who discovered this also discovered the KRACK vulnerability. The researcher noted that attacks like this can be completely avoided if security patches are installed to ensure that devices are not subject to a FragAttack.

Another interesting type of attack utilizing a feature added as part of Wi-Fi 5’s standard called MU-MIMO allows an attacker to essentially deny service to other users, slowing the network speeds of all clients on said access point. The MU-MIMO lets users share network time and spectrum resources to help increase the overall quality of what’s being delivered to a client.

Some additional research about vulnerabilities helps me understand just how many different types of failures in security there are out there. Funny enough the number of CVEs tied to memory issues like buffer overflow, out-of-bound read, or buffer over-read was quite eye-opening. In total, from the researchers of Peteris Paikens and Krisjanis Nesenbergs there were 105 of these totals still open today.

As I continue to research papers, articles and websites regarding vulnerabilities I’m trying to fit in each of these possibilities into considerations and ideas for what could help improve the wireless security landscape. It seems that it would be out of scope to, in some sense, to start inspecting vulnerabilities tied to hardware/software fallacies that are out of the scope of my initial research. However, I think they could help prove my point regarding the importance of security flaws.

References

<https://thehackernews.com/2021/05/nearly-all-wifi-devices-are-vulnerable.html>

<https://papers.mathyvanhoef.com/usenix2021.pdf>

<https://news.northeastern.edu/2025/01/09/wifi-security-vulnerability-research/>

<https://ccdcoe.org/uploads/2024/05/CyCon_2024_Paikens_Nesenbergs-1.pdf>