**Fragment and Forge: Breaking Wi-Fi Through Frame Aggregation and Fragmentation**

This paper describes how sensitive data can be exfiltrated from devices using IEEE 802.11 standards. The author also presents a tool that can be used to detect whether any device is vulnerable to these attacks and discuss countermeasures to prevent the same. These attacks are due to a design flaw in 802.11’s frame aggregation and fragmentation features. A design flaw in the fragment cache of the receiver is also demonstrated that can be used to exfiltrate sensitive data. Frame aggregation attack works on the basis of attackers being able to manipulate a Wi-Fi packet such that they are able to inject malicious frames along with legitimate frames of a packet. Frame fragmentation attack works on the principle that mixing frames encrypted under different keys and adding malicious frames during reconnect or reassociation can lead to sensitive data exfiltration. The impact of the attacks includes creating malicious DNS servers or performing port scans to conduct reconnaissance

**Strengths**

* Frame aggregation attack works on most kind of IEEE 802.11 Wi-Fi devices. From the early version WEP to the latest WPA3, all the protocols are vulnerable to this attack. This means that the attack proposed has wide implications and scope.
* The author of the paper also implements a test tool that covers more than 45 test cases and can be used to determine whether a device is vulnerable to these attacks or not.
* Countermeasures to the attacks and vulnerabilities discovered are also discussed at the end of the paper. Fragment cache attacks can be prevented by clearing the cache whenever reconnecting or associating with the network.

**Weaknesses**

* Frame aggregation attacks work only when the adversary is within the radio range of the victim receiver. So that places physical limitations on where and when the attack can be performed.
* The fragment cache poisoning attack described in the paper requires the attacker to possess valid credentials, this limits the practicality of the attack.
* The mixed key fragmentation attack works only when one or more devices send fragmented frames. The author also talks about the experimental analysis of a technique to support more devices, but that is only part of future work.
* Frame aggregation attack works only on devices that support fragmented A-MSDUs. Only 33/56 devices tested supported fragmented A-MSDUs