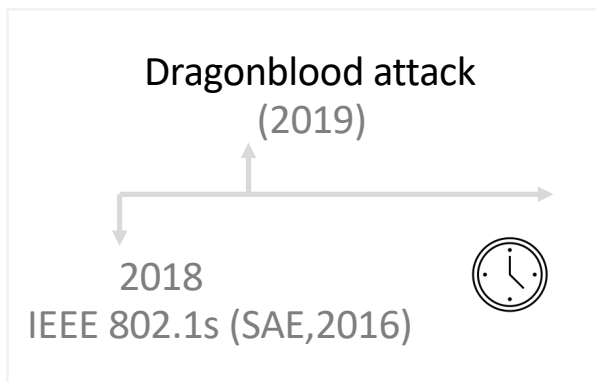







Wi-Fi Protected Access 3 (WPA3) -

<https://pagesonsecurity.blogspot.com/>



Types	Personal	
	Enterprise	
	Enterprise with 192-bit mode	

- + Better cryptography
- + Forward secrecy 
- + Management frame protection 
- + Open Wi-Fi Networks: unauth. data encryption
- Attacks: downgrade (WPA2), side-channels vs. DoS, Dragonblood, etc.

SAE: Simultaneous Authentication of Equals
 DoS: Denial of Service
 PAKE: Password Authentication Key Exchange
 EC: Elliptic Curve
 KDF: Key Derivation Function

Dragonfly Key Exchange

