* Op datalaag
* Content address memory (CAM) exhaust attack: de switch zijn tables die beslissen naar waar hij doorsluist worden geflood waardoor hij in broadcast gaat als het vol zit
* ARP: (ip omzetten naar mac): spoofing
* Dhcp starvation: blijven dhcp request sturen
* Packet overhearing: (shared medium)
* Spoofed deauthentication messages: iemand constant offline kegelen
* Hidden node: a stuurt naar iedereen dat ie naar b begint te sturen maar c is out of range van a dus weet dit niet en begint ook naar b te sturen. Voor dit te verkomen RTS request to send berichten nodig. CTS clear to send al response als het goed is. Fucking carol kan dan RTS spammen om de X aantal seconden. Dit is dus een DdoS zonder echte spamming want maar een bericht sturen omde zoveel tijd
* Security solutions: WEP / WPA / WPA2

# WEP

+ authenticatie, confidentieel, integriteit - no key management, replay attacks

* Kleine en statische sleutels: makkelijk te cracken

## Open system authentication

## Shared key authentication

## Authentication gebruik makende van SSID van AP

## MAC address filtering

AP kijkt of binnenkomende MAC in zijn lijst staat maar attacker kan als hij dit onderschept zijn MAC aanpassen.

# WPA

* Betere encryptie: intilialisatie vector is 48 bit ipv 24 bit
* Betere encryptie: 104 bit keys afhankelijk van een master secret en anders per packet: confidentialiteit
* 802.1X framework voor authenticatie + key management
* Geen replay attacks mogelijk
* Integriteitchecks

## 801.1X (authenticatie)

## 

Supplicant: draadloze client in het draadloos station

Authenticator: meestal de Access Point

Authentication server: bevat user-related authenticatie informatie

* Tot authenticatie compleet is kan de client enkel totaan de AP
* De AP kan ook aan authenticatie doen op basis van MAC adressen. Anti DDOS