1 Inledning

Det här är ett arbete om wpa2:s säkerhet och säkerhetsfrågor kring wpa2 som har uppstått kring wpa2 sen det släpptes.

1.1 Utvecklingen till WPA2

Jag kommer att ta upp hur wpa2:s säkerhet fungerar och om hur det utvecklades till det som används idag. Och säkerheten I de olika versionerna av wpa2 och var och varför de används där.

1.2 Säkerhet kring WPA2

Runt säkerhetsfrågorna tar jag upp risker I wpa2:s säkerhet och hål I säkerheten som uppstått I wpa2:s säkerhet. Kommer också att diskutera framtida utveckling av wpa2. Utvecklingen för att ta itu med riskerna och hålen som hittats I wpa2:s säkerhet. Kommer också diskutera utvecklingen av nya säkerhetsprotokoll som börjats pga utvecklingarna I nätkommunikation.

2 Wpa2

I den här delen kommer jag att gå in på hur WPA2 uppdaterades från WEP och WPA, och varför det behövdes uppdateringarna i säkerhets protokollen och i WPA. Kommer också att gå in på hur WPA2 fungerar och hur WPA2:s olika versioner fungerar och varför de används så.

2.1 Från WEP till WPA2

WEP var det första säkerhets protokollet för Wi-Fi. WEP började användas 1999 när det första standarden, 802.11b, för Wi-Fi kom ut. WEP började användas för att göra Wi-Fi nät kommunikation lika säkert som en nät kommunikation som är kopplad med kabel. Problemet med WEP var krypteringsnyckeln. Eftersom WEP använde sig av bara en nyckel mellan alla som var kopplade, blev det möjligt att lösa krypteringen bara med att fånga tillräckligt många paket. Och 2001 kom en analys utav WEP som visade att man kan få fram WEP nyckeln på bara några minuter.
WPA kom ut runt 2002 som en uppföljning till WEP för att täcka de stora hålen i WEP:s säkerhet. WPA utvecklades så att det kunde användas på hårdvara som använde WEP tidigare för att göra övergången så lätt som möjligt. Största ändringen mellan WEP och WPA var krypteringsnyckeln. Istället för att använda en statisk nyckel som i WEP användes en TKIP kryptering. Alltså man skickar en ny krypteringsnyckel med varje paket istället för samma nyckel varje gång.
Och istället för att skicka en 128-bit nyckel använder man sig av en 258-bits nyckel.
Till WPA utvecklades två olika version, WPA-Personal och WPA-Enterprise. WPA-Personal är menat för privata användare, alltså vanliga kunder, personer.

Till WPA-Personal använder man sig av en PSK. PSK är en personlig nyckel man använder för att logga in på nätverket, alltså ett lösenord till routern.
WPA-Enterprise är menat för företag eller grupper som alla använder samma nätverk. Inte då menat som ett öppet nätverk som man kan hitta på ett kafe eller liknande, utan för företag som vill ha ett säkert nätverk för sina arbetare.
WPA-Enterprise använder sig inte av en PSK utan av RADIUS kryptering för att komma in på nätverket. RADIUS är ett inloggningssystem till nätverket. En PSK som bara är ett lösenord till routern medan RADIUS är med ett personligt användarnamn och lösenord per arbetare till nätverket. Eftersom WPA bara kom ut som en temporär lösning till WEP:s stora säkerhetsproblem började man utveckla WPA2. WPA2 utvecklades så att det stöder hela IEEE 802.11i säkerhets protokollet som kom ut 2004.

2.2 WPA2:s säkerhet

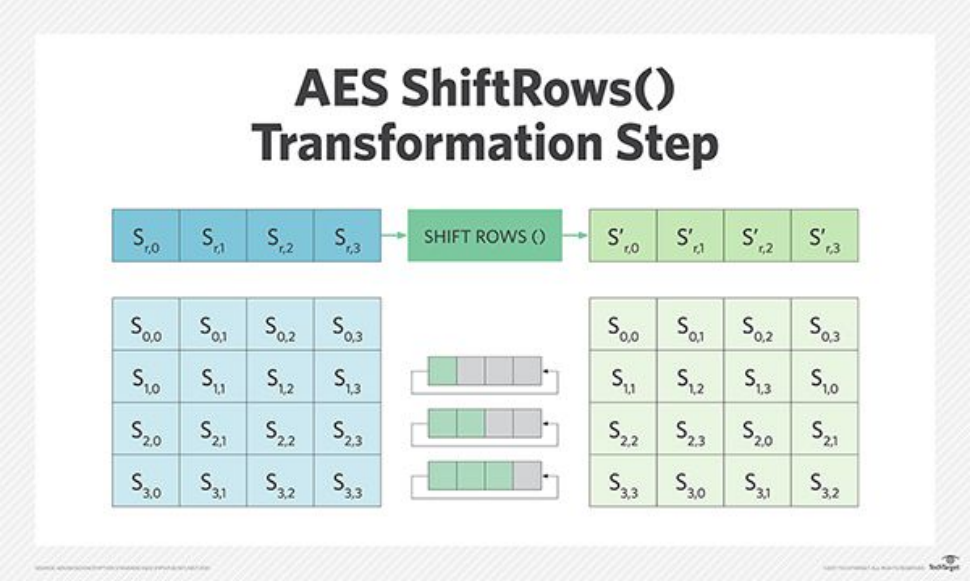
Eftersom WPA utvecklades som en snabb lösning till WEP fungerade det med samma hårdvara som WEP, medan WPA2 utvecklades som en långvarig lösning. Det här gjorde att man behövde bättre hårdvara än vad man behövde till WPA och WEP. De ökade kraven på hårdvaran till WPA2 beror på de hårdare krypteringarna som sattes till WPA2, så att WPA2 stöder IEEE 802.11i säkerhets protokollet. De nya krypteringarna behövde mera processerings kraft än vad den gamla hårdvaran kunde använda.
Ändringarna från WPA som gjordes var att man ersatte TKIP och RC4 krypteringen i WPA med en AES kryptering och började använda CCMP protokollet.

2.2.1 AES, Advanced Encryption Standard

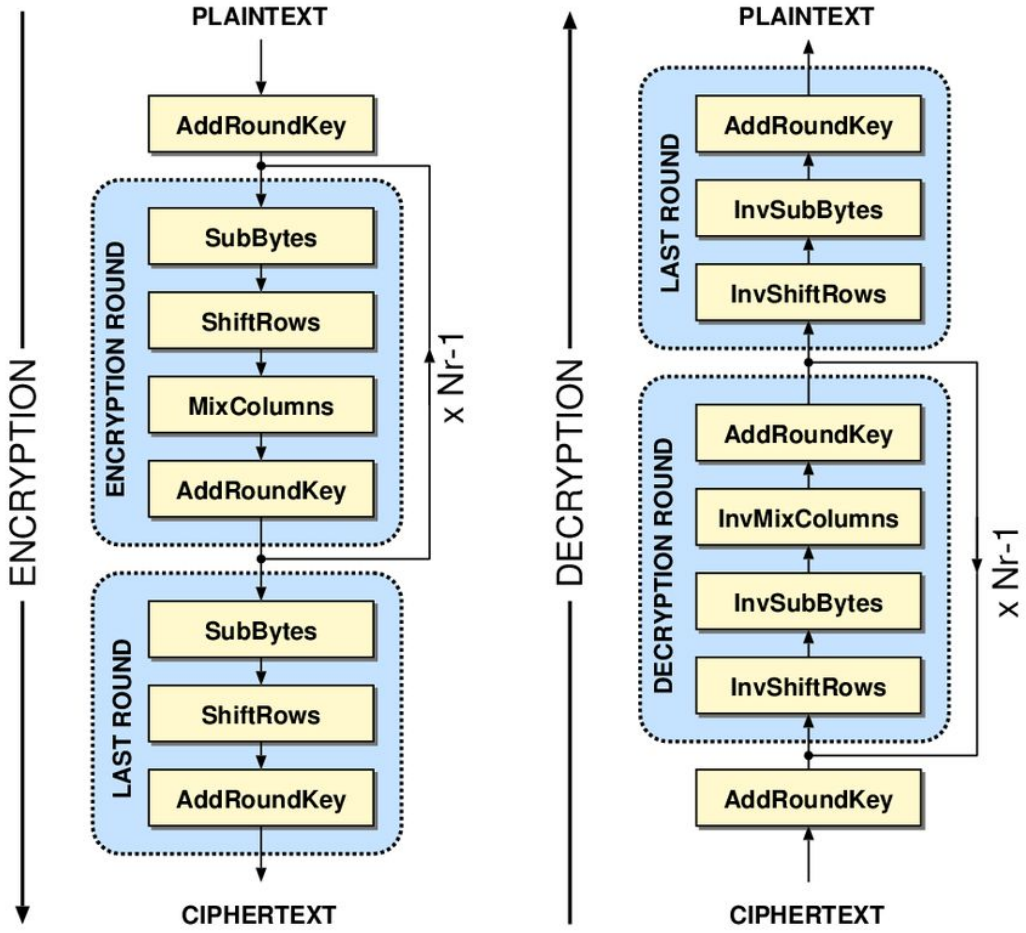
AES är krypteringsalgoritm som utvecklades av Joan Daemen och Vincent Rijmen, och den blev standard för kryptering 2001. AES fungerar som en 128-bitars block chiper, och kan använda 128-,192- eller 256-bit längds nyckel för

kryptering. För att kryptera och dekryptera meddelanden använder man sig av substitutioner och permutationer blockvis som har längden 128-bit. Beroende på längden av krypteringsnyckeln behöver man olika många iterationer av blocket. För längden 128-bit krypteringsnyckel krävs 10 iterationer och längden 192-bit kräver 12 iterationer och 256-bit 14. En iteration består av fyra steg:

1. Det första steget är substitution. Man byter ut alla bits i en array enligt en tabell.
2. Andra steget är rad förflyttning. Varje rad flyttar sig ett eller flera steg till vänster.



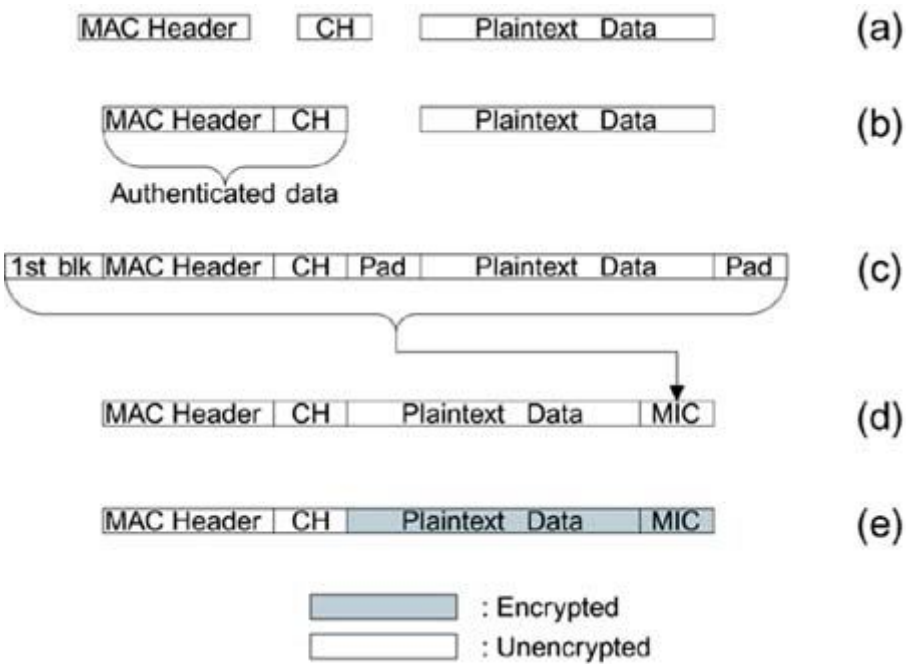
3. Tredje steget är kolumn blandning. Man blandar om kolumnerna som en matrix multiplikation.
4. Sista steget är att man använder sig av krypteringsnyckeln för att göra en exklusiv disjunktion. En logisk funktion för att veta vad som ska med.



2.2.2 CCMP, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol

CCMP är säkerhets protokollet som började användas för att hålla upp standarden till IEEE 802.11i kraven. CCMP är ett krypteringsprotokoll som används med AES eftersom AES tar emot block av längden 128-bits. Ett krypterat meddelande med CCMP protokollet består av några saker. En MAC-adress, CCMP-nyckel,

krypterade meddelande och en MIC-nyckel. MAC-adress, Media Access Control address, är en identifierare till sändaren och mottagaren. MAC adressen är unik till alla nätverkskort vilket gör att den är specifik till alla datorer. CCMP-nyckeln består av en 48-bit paket nummer, som är till för att skydda mot replay-attacker, och är unik för varje paket man skickar. MIC-nyckeln som består av CCMP-nyckeln, MAC-adressen och annat data från meddelande som sedan körs genom AES krypteringen för att få en 128-bit krypteringsnyckel. Men MIC-nyckeln man behöver är bara 64-bit lång så man man använder de högre 64-bits av resultatet.



2.3 WPA2:s olika versioner

Som till WPA utvecklades det två olika versioner, WPA2-PSK och WPA2-enterprise.

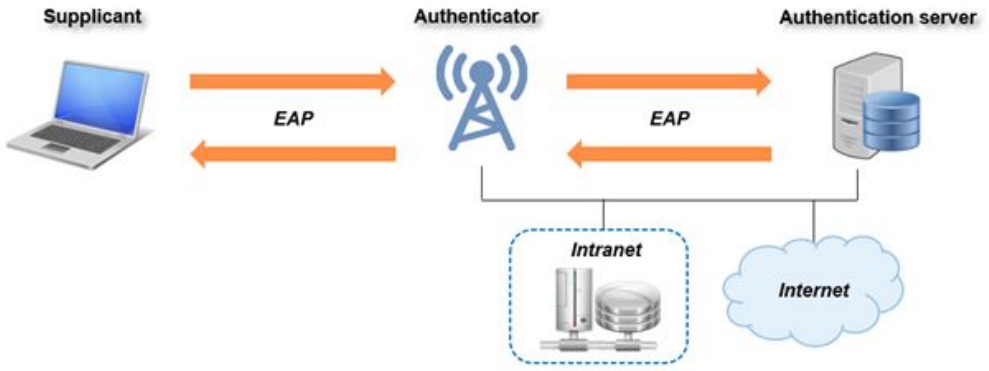
2.3.1 WPA2-PSK

WPA2-PSK, Pre-Shared Key, är det som man använder i hemmet.
PSK:n är lösenordet till Wi-Fi:n så att man slipper in på det. PSK:n är alltså samma för alla maskiner som ska ansluta till nätverket. PSK används sedan för att skapa PMK, Pairwise Master Key, som används i CCMP och AES krypteringen.

2.3.2 WPA2-Enterprise

WPA2-Enterprise är gjort för mera företags platser där det är flera som ska komma in på samma nätverk. Eftersom en PSK som delas med alla arbetare som i sin tur kan dela den med vem som helst, och gamla arbetare som fortfarande har sina maskiner kopplade till nätet inte är säkert för företag som vill hålla sin nätverkstrafik säker. För att använda WPA2-Enterprise behöver man en RADIUS server. RADIUS, Remote Authentication Dial In User Service, är en server som pratar med routern med EAP, Extensible Authentication Protocol, för att släppa in maskiner till nätverket. För att slippa in på ett WPA2-Enterprise nätverk behöver man inloggnings-namn och lösenord, som är personliga för alla som ska slippa in på nätverket. Istället för som i WPA2-PSK där det är lösenordet som är det som

skapar PMK är det servern som skapar den unika nyckeln för CCMP och AES krypteringen.



2.3.3 WPA2-PPSK

3 WPA2 säkerhetsproblem

Som alltid finns det säkerhetsrisker. Sen WPA2 kom ut har det varit svårare att komma in på nätverk än tidigare men till WPA2 har det också hittats problem. Det vanligaste problemet är förstås att man sitt lösenord till nätverket eller det att man använder ett så lätt lösenord att man kan gissa det utan att behöva göra något annat. I oktober 2017 publicerades detaljer för en KRACK attack som hittades av Mathy Vanhoef och Frank Piessens.

3.1 WPA2-PSK problem

KRACK attacken som går att använda mot alla WPA2-PSK säkerheter har man kunnat komma in på ett WPA2 nätverk tidigare.

3.2 WPA2-Enterprise problem