# Fördjupning ”accessäkerhet i WiFi”

## Översikt:

### WEP

WEP – Wired Equivalent Privacy. Den äldsta säkerhetsfunktionen – lanserades samtidigt som de första komersiella standarderna för WiFi – i slutet av 90-talet. Tanken är att ”emulera” ett ”rör”, så som om enheten är anslutet i ett Ethernet-LAN och att datat inte kan avlyssnas utifrån. Detta görs med ett (rudimentärt) kryptologiskt skydd (med en 40 bitar lång pre-shared-key) RC4-krypto.

### WPA

WPA- WiFi Protected Access. En betydligt säkrare metod som använder TKIP (Temporal Key Integrity Protocol) vilket ändrar sina kryptonycklar \_dynamiskt\_ under tiden det används.

### WPA2

Använder – i stället för RC4 – AES (Advanced Encryption Standard) – ett välanvänt kryptosystem ursprungligen utvecklat av USAs handelskammare för att säkra system som betalningssystem och liknande för tiden för dess tillkomst. TKIP ersattses med CCMP.

### WPA3

Släpptes 2018 och är den senaste versionen av WPA.

### WPS

WPS – WiFi Protected Setup. En ny standard för att accessa WiFi-nätverk, utvecklat med användarvänlighet som primärt fokus. Mojängen ansluts med antingen hårdvaruknapptryck, med PIN eller i vissa fall QR-kod eller liknande. Mojänger som ansluts med WPS är kryptologiskt skyddade, men då många mojänger idag har stöd för WPS (där den primära säkerhetsmekanismen är fysisk access till routern/AP) behövs ofta olika tilläggsskydd i form av MAC-adressfiltrering eller liknande.

Medialänk: <https://youtu.be/WZaIfyvERcA>

## WEP:

WEP – Wired Equivalent Privacy – är en del av de ursprungliga 802.11-standarderna och är tänkt – precis som WiFi rent generellt – att vara jämförbart med en kabelansluten LAN-koppling av samma tidsera. Precis som med de ursprungliga kraven på accessens bandbredd (som då var ungefär lika snabbt som de 10 Mbps LAN som var gängse standard) ville man få en ”virtuell kabel” som inte gick att avlyssna i radioetern.

Till skillnad från trådade nätverk kan (ju) trafiken på ett trådlöst nätverk över radio avlyssnas i klartext av vem som helst som har någorlunda fysisk närhet till själva nätverket (är ”i täckning”).

WEP var tänkt att lösa de här problemen genom att införa ett system både för autenticering av klienten och skapa en avlyssningssäker ”tunnel” mellan klient och AP.

WEP använder RC4 som symmetriskt blockkrypto som kryptoalgoritm och i komersiella, internationella (utanför USA) sammanhang 40 bitar för-utdelad (Pre-Shared) nyckel. (I USA var nyckellängden 104 bitar). Som ”Salt” eller ”Initialiseringsvektor” för att räkna ut datakryptot för själva användartrafiken lades det på 24 slumpmässiga bitar för att räkna ut datakryptonyckeln.

WEP stödde från början två autenticeringsmetoder – ”Shared Key Authentication” (SKA) och ”Open systems Authentication” (OSA).

Användare autenticeras med ett ”four way handshake”.

* 1: Client Authentication Request skickas till AP
* 2: AP skickar “challenge text” tillbaka till klienten
* 3: Klienten krypterar ”challenge text” med sin förinställda nyckel och skickar tillbaka det krypterade meddelandet till AP
* 4: AP kontrollerar om meddelandet är korrekt och vid gynnsamt utfall – autenticerar användaren på nätet.
* (5: Användaren ansluter med sin mojäng till nätet).

Häri ligger det stora problemet med autenticeringssäkerheten av användaren. Både ”challenge text” – som AP skickar i klartext för att göra själva challengen av anslutningen, och det krypterade svaret kommer att gå i klartext över \_hela\_ nätverket (då klienten inte ännu är autenticerad och ansluten). Det görs att klartext och kryptotext skickas ”tillsammans” och kan bägge avlyssnas. Att dekryptera meddelandet när man har både klartext och kryptotext och kan jämföra dessa med varandra är – förhållandevis ”enkelt” med lite kunskaper om vilket system som använts för att kryptera datat med (i det här fallet RC4).

Det stora problemet i WEP är emellertid inte (endast) med autenticeringsmetoden. Eftersom man använder RC4 (symmetrisk ström) kan man jämföra två krypterade meddelanden med varandra och därigenom ”gissa” nyckeln, då nyckellängden inte är speciellt lång och ”saltet” (som man tillför kryptoalgoritmen för att få ett mer slumpmässigt resultat) är endast 24 bitar. Genom att lyckas träffa rätt i gissningen av bara 24 bitars ”salt” har man extraherat kryptonyckeln och kan lätt dekryptera den krypterade trafiken.

Medialänk: <https://youtu.be/6s101qYUopc>

## WPA

WPA – WiFi Protected Access – är en standard som från början var ett frivilligt öppet projekt för att öka säkerheten i trådlösa nätverk i skenet av att WEP (som var standardiserat av IEEE redan i de första IEEE 802.11-standarderna) ansågs osäkert rätt tidigt. De första användbara versionerna av WPA kom runt 2002, även om standarderna i sig själv funnits några år tidigare.

Ett access-säkerhetsrelaterat problem med WEP som gjorde att man började titta på en ny standard var att WEP gjorde att samtliga användare på samma WiFi-LAN kunde ”se” eller ”höra” varandra, så snart de var anslutna i samma nätverk. Tänk på detta som ett ”hubbat” nätverk eller ett ”repeater”-nätverk av Ethernettyp. Det stämmer rätt bra in på ambitionen att på 90-talet ha ett trådlöst nät ”av samma eller jämförbar standard” som dåtidens kabelbundna nätverk.

En av grundtankarna med accessmetodiken för WPA var att skapa enskilda ”kanaler”, ”rör” eller ”tunnlar” med varje enskild ansluten enhet – som i ett ”switchat” eller ”bryggat” nätverk (där ju enheterna inte kan se bortom sin egen kollisionsdomän i Ethernet).

Medialänk: <https://youtu.be/WI6NHQGc1Is>

WPA använder RC4 med TKIP (Temporal Key Integrity Protocol). Saltet/Initialiseringsvektorn är (betydligt) större än hos WEP och är krypterat. Varje paket krypteras individuellt, med en ny nyckel – i stället för med WEP där paketen krypteras i en ström med samma nyckel.

Tanken med WPA var att du ska kunna använda TKIP som en ”mellanstandard” mellan WEP och ”vad som kommer sen”, mest för att snabbt få en standard till stånd som löste de mest akuta problemen med WEP med i samma hårdvara som använde WEP, utan att behöva uppgradera själva routrarna eller de nätverkskort som fanns i handeln för WiFi på den tiden. WPA kallas därför ibland för ”den temporära WPA”.

## WPA2

WPA2 kom 2005 och här hade man tänkt om standarden från grunden. Man hade bytt ut det gamla (och knäckta) RC4-kryptosystemet mot AES (Advanced Encryption Standard). För säker nyckelutväxling byttes TKIP ut mot CCMP (Counter mode Cipher block chaining Message authectication code Protocol).

De nya kryptoalgoritmerna och nyckelöverföringsprotokollen krävde betydligt kraftigare (och dyrare) hårdvara, då de tog märkbart fler CPU-cykler i anspråk för sina nyckelberäkningar. WPA2 använder 128 bitars nyckellängd.

### WPA2 ”Enterprise” / 802.1x

Denna uppsättning medger att du integrerar inloggningsförfarandet med Radius eller LDAP till redan existerande användarstrukturer (som till ett företags interna LAN)

Medialänk: <https://youtu.be/DspgyuedICM>

### WPA3

WPA2 knäcktes med ”KRAK-buggen” 2017.

WPA2 använder 128 bitars krypto i konsumenthårdvara – vilket även WPA3 gör. (Det finns stöd för att köra nyckellängder upp till 192 bitar i WPA3, men man anser generellt att det inte – med Moores Lag – kommer att öka säkerheten över tid.)

Då förlänga nyckellängd eller kryptologisk data egentligen inte försvårar knäckandet (det tar bara längre tid) har man i WPA3 koncentrerat sig på hur man praktiskt kan öka säkerheten, men utan att ändra kryptostandarderna (som ändå är kända).

Man introducerar en andra linjens försvar mot användare/nätverk som fortfarande använder svaga lösenord. En av dessa standarder heter SAE (Simultanous Authentication of Equals). Tanken med SAE är att skapa ett system där användarens data inte längre kan dekrypteras genom att spelas in och i efterhand kryptoanalytiskt ”knäckas” genom någon form av ”brute force”-attack mot användarens lösenord. Själva kryptot gäller bara en gång och bara under tiden som trafiken är ”i luften”.

Medialänk: <https://youtu.be/aPoe4WtX2mU>

## IEEE 802.1x -EAP Extensible Authentication Protocol

IEEE802.1x – EAP är en standard för att kontrollera nätverksåtkomst – ursprungligen utformat för switchade nätverk. Det stora problemet för moderna switchade Ehernet-LAN är att vem som helst som har fysisk access till en switchport är ”på insidan” av nätverket och har där kunnat beredas åtkomst till nätverkets alla resurser.

EAP utvecklades från början för att på olika sätt introducera ”port security” i switchar – funktioner för att kontrollera att det som kopplades in i switchen faktiskt var något som skulle beredas åtkomst i nätverket.

I sin enklaste form kan EAP beredas att kontrollera en enhets MAC-adress för att kontrollera att enheten faktiskt får ansluta till nätverket. Andra kontrollfunktioner kan vara att enheten har ett kryptocertifikat och/eller nyckel eller att användaren avkrävs användarnamn och lösenord. Detta kan kontrolleras med protokollen RADIUS och/eller LDAP och beroende på utvärderingen av användarens olika ”cridentials” ges olika - eller en ”skiktad” om man så vill – åtkomst till nätverket. Om en användare t.ex. \_har\_ ett konto i nätverket \_men\_ saknar (giltiga) certifikat för en tjänst kommer användaren bara åt vissa delar av nätverket, medan en användare som har samtliga kontrollfunktioner installerade kommer åt allt i nätverket.

Medialänk: <https://youtu.be/bwUB2C2i_H0>

I WiFi-sammanhang har detta använts på olika sätt framförallt i olika ”publika” WiFi-LAN. Ett av de mest kända i Sverige var Telia Homerun där man på olika sätt hade försett Telia-abbonenters telefoner med certifikat samt registrerat deras MAC-adresser. En Telia-användare blev då ”automagiskt” och ”gratis” uppkopplad överallt där det fanns en ”hotspot” för Homerun. Andra användare – som var abbonenter i andras telenät (som Telenor och Tre) kunde köpa en (begränsad) access, genom att köpa vouchers, ”skraplotter med engångskoder” etc. för att beredas tillgång till nätet.

Inom företagsnät har standarden ofta använts för att skikta nätet i ”publika” delar (BYOD eller gästnätverk) och privata, men i samma fysiska nätverksstruktur.

Medialänk: <https://youtu.be/m7NkBFCm9Tk>

## Fördjupning/trender/knyta ihop säcken:

Alla de här standarderna och deras styrkor och svagheter kommer emellertid inte till någon nytta i något sammanhang om man inte förstår hur de samverkar och vad de kan användas till tillsammans.

Ofta kör inget företag bara en standard utan en kombination (t.ex. av WPA2 enterprise och 802.1x) för att ansluta användarna och använder då olika standarder beroende på hur utvärderingen av användarens anslutning sett ut.

En stor trend man sett de senaste åren är att man fokuserat mindre i moderna säkerhetslösningar (som WPA3 och 802.1x) på praktiker som går ut på att skydda nätverket tekniskt (med mer komplexitet i kryptosystemen som skyddar dataintegriteten, större MAC-adressfilter etc.) och i stället inriktat sitt fokus mer kring användaren och hens användande av nätverksresurserna. De ”mjuka” sakerna som rör fysiskt säkerhetsskydd av t.ex. inloggningstoken, större komplexitet på lösenord, hur ofta lösenorden byts, att inte samma lösen används överallt – har fått ett allt större fokus.

Det här är en trend vi sett i stort inom IT-säkerhetsbranchen – framförallt under 2020 och 2021 pga den rådande situationen med Corona – att man går från ett fokus på ökad teknisk komplexitet för att skydda nätverket – och i stället försöker hjälpa användarna att skydda sina personliga cridentials och eller den data man måste använda i sitt dagliga arbete – med hjälp av t.ex. olika säkerhetspolicies och efterlevnad av dessa.

Medialänk: <https://www.youtube.com/watch?v=XOnwMzlt2os>